

Astaro Security Gateway

(Version 7.505)

Administration Guide

Date: 2010-05-04 17:08 UTC

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of Astaro AG. Translations of this original manual must be marked as follows: "Translation of the original manual".

© 2000–2010 Astaro GmbH & Co. KG. All rights reserved.

An der RaumFabrik 33a, 76227 Karlsruhe, Germany

<http://www.astaro.com/>

Astaro Security Gateway, Astaro Mail Gateway, Astaro Web Gateway, Astaro Command Center, Astaro Gateway Manager, and WebAdmin are trademarks of Astaro AG. Cisco is a registered trademark of Cisco Systems Inc. iPhone is a trademark of Apple Inc. All further trademarks are the property of their respective owners.

Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to <documentation@astaro.com>.

Table of Contents

1	Installation	1
	Recommended Reading	1
	System Requirements	2
	UPS Device Support	3
	RAID Support	4
	Installation Instructions	4
	Basic Configuration	8
	Backup Restoration	13
2	WebAdmin	15
	WebAdmin Menu	16
	Button Bar	17
	Lists	17
	Dialog Boxes	18
	Buttons and Icons	19
	Group Tooltips	20
3	Dashboard	23
4	Management	27
	System Settings	28
	Organizational	28
	Hostname	28
	Time and Date	28
	Shell Access	31
	Reset Configuration or Passwords	31
	WebAdmin Settings	32
	General	32
	Access Control	33
	Security	34
	HTTPS Certificate	34
	User Preferences	36
	Licensing	37
	OnDemand Licensing	38
	Classic Licensing	40
	Overview	41
	Installation	42
	Active IP Addresses	43
	Up2Date	44

Overview	44
Configuration	47
Advanced	47
Backup/Restore	48
Backup/Restore	49
Automatic Backups	50
V6 Backup Import	51
User Portal	53
Global	54
Advanced	55
Notifications	57
Global	57
Notifications	57
Advanced	58
Customization	58
Global	58
HTTP/S Proxy	60
Download Manager	61
SMTP/POP3 Proxy	62
SNMP	62
Query	63
Traps	65
Central Management	67
Astaro Command Center	67
Setting up ACC V2.0	68
Setting up ACC V1.4	69
ACC Objects	70
Live Log	72
High Availability	72
Hardware and Software Requirements	73
Status	74
System Status	75
Configuration	76
Shutdown and Restart	82
5 Users	83
Users	83
Groups	86
Authentication	89
Global Settings	89
Servers	91

eDirectory	91
Active Directory	93
LDAP	96
RADIUS	98
TACACS	100
Single Sign-On	102
Advanced	104
6 Definitions	107
Networks	107
Services	111
Time Events	114
7 Network	117
Interfaces	117
Interfaces	118
Automatic Interface Network Definitions	119
Interface Types	119
Ethernet Standard	121
Ethernet VLAN	122
Cable Modem (DHCP)	124
DSL (PPPoE)	126
DSL (PPPoA/PPTP)	127
Modem (PPP)	129
Additional Addresses	131
Link Aggregation	132
Uplink Balancing	133
Multipath Rules	136
Hardware	137
Bridging	138
Status	138
Advanced	140
Static Routing	141
Standard Static Routes	141
Policy Routes	142
Dynamic Routing (OSPF)	144
Global	144
Interfaces	145
Area	147
Message Digests	149
Debug	150

Advanced	150
Quality of Service (QoS)	151
Status	151
Traffic Selectors	153
Bandwidth Pools	155
Multicast Routing (PIM-SM)	156
Global	157
Interfaces	158
RP Routers	159
Routes	160
Advanced	161
Uplink Monitoring	162
Global	162
Actions	162
Advanced	163
8 Network Services	165
DNS	165
Global	165
Forwarders	166
Request Routing	166
Static Entries	167
DynDNS	167
DHCP	170
Servers	170
Relay	172
Static MAC/IP Mappings	173
Lease Table	174
NTP	175
9 Network Security	177
Packet Filter	177
Rules	177
ICMP	181
Advanced	182
NAT	185
Masquerading	186
DNAT/SNAT	187
Intrusion Prevention	189
Global	189
Attack Patterns	191

Anti-DoS/Flooding	193
Anti-Portscan	195
Exceptions	197
Advanced	199
Server Load Balancing	200
Balancing Rules	201
Advanced	202
Generic Proxy	202
SOCKS Proxy	203
IDENT Reverse Proxy	204
10 Web Security	207
HTTP/S	208
Global	208
AntiVirus/Malware	211
URL Filtering	213
URL Filtering Categories	217
Exceptions	218
Advanced	220
HTTPS CAs	225
HTTP/S Profiles	229
Overview	230
Proxy Profiles	231
Filter Assignments	234
Filter Actions	236
FTP	239
Global	239
AntiVirus	240
Exceptions	241
Advanced	243
11 Mail Security	245
SMTP	245
Global	245
Routing	246
AntiVirus	249
AntiSpam	253
Exceptions	259
Relaying	260
Advanced	263
SMTP Profiles	265

POP3	270
Global	271
AntiVirus	272
AntiSpam	273
Exceptions	275
Advanced	277
Encryption	280
Global	283
Options	285
Internal Users	286
S-MIME Authorities	289
S-MIME Certificates	291
OpenPGP Public Keys	292
Quarantine Report	293
Global	295
Exceptions	296
Advanced	298
Mail Manager	299
Mail Manager Window	300
SMTP/POP3 Quarantine	300
SMTP Spool	302
SMTP Log	303
Global	304
Configuration	306
12 RED Management	309
Global Settings	310
Device Configuration	311
What is RED?	313
13 VoIP Security	315
SIP	315
H.323	316
14 IM/P2P	319
Settings	319
Global	319
Advanced	320
Instant Messaging (IM)	321
Protocols	321
Exceptions	323
Peer-to-Peer (P2P)	324

Protocols	325
Exceptions	326
15 Site-to-site VPN	329
IPSec	330
Connections	332
Remote Gateways	333
Policies	336
Local RSA Key	339
Advanced	341
Debug	344
SSL	344
Connections	344
Settings	347
Advanced	349
Certificate Management	351
Certificates	351
Certificate Authority	353
Revocation Lists	355
Advanced	356
16 Remote Access	357
SSL	358
Global	358
Settings	360
Advanced	361
PPTP	363
Global	363
iPhone	365
Advanced	366
L2TP over IPSec	367
Global	367
iPhone	371
Advanced	372
IPSec	373
Connections	375
Policies	377
Advanced	380
Debug	383
Cisco VPN Client	383
Global	383

iPhone	385
Debug	386
Advanced	386
Certificate Management	387
Certificates	387
Certificate Authority	388
Revocation Lists	388
Advanced	388
17 Logging	389
Settings	389
Local Logging	389
Remote Syslog Server	391
Remote Logfile Archives	393
View Log Files	395
Today's Log Files	395
Archived Log Files	396
Search Log Files	397
18 Reporting	399
Settings	399
Settings	399
Exceptions	400
Anonymizing	401
Hardware	402
Daily	402
Weekly	403
Monthly	403
Yearly	404
Network Usage	404
Daily	404
Weekly	405
Monthly	405
Yearly	406
Accounting	406
Network Security	407
Daily	407
Weekly	408
Monthly	408
Yearly	408
Packet Filter	408

IPS	409
Web Security	410
Web Usage	410
Blocked Usage	411
IM	412
P2P	412
Deanonymization	412
Mail Security	413
Usage Graphs	413
Mail Usage	414
Blocked Mail	414
Deanonymization	414
Executive Report	416
View Report	416
Archived Executive Reports	416
Configuration	416
19 Support	417
Manual	418
Contact Support	418
Tools	419
Ping Check	419
Traceroute	420
DNS Lookup	421
Advanced	422
Process List	422
Local Network Connections	422
Routes Table	422
Interfaces Table	422
Config Dump	422
Resolve REF	423
A Glossary	425
List of Figures	435
Index	443

Chapter 1

Installation

This section provides information on installing and setting up Astaro Security Gateway on your network. The installation of Astaro Security Gateway proceeds in two steps: first, installing the software; second, configuring basic system settings. The initial setup required for installing the software is performed through a console-based installation menu. The final configuration can be performed from your management workstation through the web-based administrative interface of Astaro Security Gateway called *WebAdmin*. Before you start the installation, check if your hardware meets the minimum system requirements.

Note – If you are employing an Astaro Security Gateway Appliance, you can skip the following sections and directly jump to the Basic Configuration section, as all Astaro Security Gateway Appliances ship with ASG Software preinstalled.

The following topics are included in this chapter:

- Recommended Reading
- System Requirements
- Installation Instructions
- Basic Configuration
- Backup Restoration

Recommended Reading

Before you begin the installation, you are advised to read the following documents that help you setting up Astaro Security Gateway, all of which are enclosed within the package of your Astaro Security Gateway Appliance unit and which are also available at Astaro's knowledgebase¹:

¹ <http://www.astaro.com/kb/>

- Getting Started Guide
- Operating Instructions

System Requirements

The minimum hardware requirements for installing and using ASG are as follows:

- **Processor:** Pentium 4 with 1.5 GHz (or compatible)
- **Memory:** 1 GB RAM
- **HDD:** 20 GB IDE or SCSI hard disk drive
- **CD-ROM Drive:** Bootable IDE or SCSI CD-ROM drive
- **NIC:** Two or more PCI Ethernet network interface cards
- **NIC (optional):** One heart-beat capable PCI Ethernet network interface card.

In a high-availability system, the primary and secondary system communicate with one another through so-called heart-beat requests. If you want to set up a high-availability system, both units need to be equipped with heart-beat capable network interface cards.

- **USB (optional):** One USB port for communications with a UPS device
- **Switch (optional):** A network device that connects (and selects between) network segments.

Note that this switch must have jumbo frame support enabled.

Astaro provides a list of hardware devices compatible with ASG Software. The *Hardware Compatibility List* (HCL) is available at Astaro's knowledgebase². To make the installation and operation of ASG Software less error-prone, you are advised to only use hardware that is listed in the HCL. The hardware and software requirements for the client PC used to access WebAdmin are as follows:

- **Processor:** Clock signal frequency 1 GHz or higher
- **Browser:** Firefox 2 (recommended) or Microsoft Internet Explorer 6 or 7. JavaScript must be enabled. In addition, the browser must be configured

² <http://www.astaro.com/kb/>

not to use a proxy for the IP address of the ASG's internal network card (eth0).

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100/portal/>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the Trusted Sites Zone when using Internet Explorer 7.

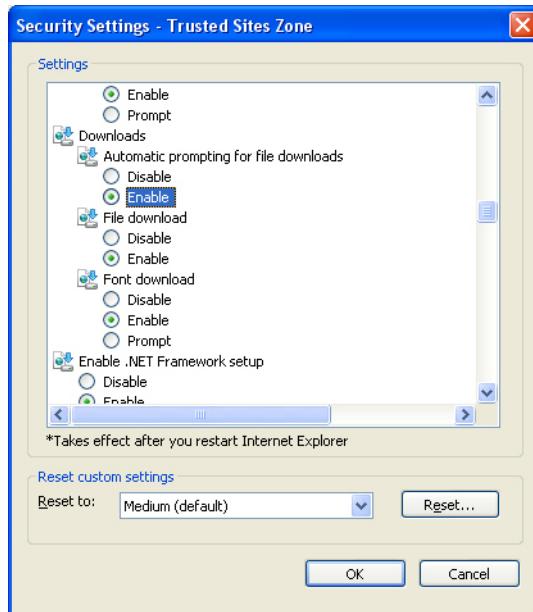


Figure 1.1 IE7 Security Settings Trusted Sites Zone

UPS Device Support

Uninterruptible Power Supply (UPS) devices maintain a continuous supply of electric power to connected equipment by supplying power from a separate source when utility power is not available. Astaro Security Gateway supports

UPS devices of the manufacturers MGE UPS Systems and APC. The communication between the UPS device and Astaro Security Gateway is made via the USB interface.

As soon as the UPS device runs in battery operation, a notification is sent to the administrator. If the power failure persists for a longer period and the voltage of the UPS device approximates a critical value, another message will be sent to the administrator—the Astaro Security Gateway will be shut down automatically.

Note – Please read the operation manual of the UPS device to connect the devices to Astaro Security Gateway. The security system will recognize the UPS device when booting via the USB interface. Only boot Astaro Security Gateway when you have connected the USB interfaces to each other.

RAID Support

A RAID (Redundant Array of Independent Disks) is a data storage scheme using multiple hard drives to share or replicate data among the drives. To ensure that the RAID system is detected and properly displayed on the Dashboard, you need to use a RAID controller that is supported by Astaro Security Gateway. Check the *hardware compatibility list* (HCL) to figure out which RAID controllers are supported. The HCL is available at Astaro's knowledgebase³. Use "HCL" as search term to locate the corresponding page.

Installation Instructions

What follows is a step-by-step guide of the installation process of Astaro Security Gateway Software.

Before you begin the installation, please make sure you have the following items available:

- The Astaro Security Gateway CD-ROM
- The license key for Astaro Security Gateway

The setup program will check the hardware of the system, and then install the software on your PC.

³ <http://www.astaro.com/kb/>

Caution – The installation process will delete all data on the hard disk drive.

1. Boot your PC from CD-ROM drive.

Select the appropriate installation mode for your computer. Three pre-compiled kernel options are available for this purpose:

- **default:** Kernel for systems with one or more processors (SMP).
- **nosmp:** Kernel for systems with one processor—boots without SMP support, i.e. multiple CPUs will not be supported.
- **classic:** Kernel for systems with one CPU, in which the support for SMP, APIC (Advanced Programmable Interrupt Controller) and ACPI (Advanced Configuration and Power Interface) is disabled. Since in older hardware components APIC and ACPI are often not supported, we recommend using the classic kernel in this case.

2. Key functions during installation.

In order to navigate through the menus, use the following keys (please also note the additional key functions listed in the turquoise bar at the bottom of the screen):

- **Esc key:** Abort the installation.
- **Cursor keys:** Use these keys to navigate through the text boxes (for example, the license agreement or when selecting a keyboard layout).
- **Tab key:** Move back and forth between text boxes, lists, and buttons.
- **Enter key:** The entered information is confirmed, and the installation proceeds to the next step.

After selecting the installation mode, confirm the security question that follows by pressing the F8 key.

3. Confirm software installation.

Press F8 to install the provided software or Esc to abort the installation.

4. Select your keyboard layout.

Use the Cursor keys to select your keyboard layout and press Enter to continue.

5. Confirm hardware detection.

The software will check the following hardware componentshardware de-tention:

- CPU
- Size and type of hard disk drive
- CD-ROM drive
- Network interface cards
- IDE or SCSI controllers

If your system does not meet the minimum requirements, the installation will report the error and abort.

6. Select your area.

Use the Cursor keys to select your area and press **Enter** to confirm.

7. Select your time zone.

Use the Cursor keys to select your time zone and press **Enter** to continue.

8. Set date and time.

Next, enter the current date and time. Use the Tab key and the Cursor keys to switch between text boxes. Invalid entries will be rejected.

Confirm your settings with the **Enter** key.

9. Select an internal network card.

In order to use the WebAdmin tool to configure the rest of Astaro Security Gateway, select a network interface card to be the internal network card (*eth0*). Choose one of the available network cards from the list and confirm your selection with the **Enter** key.

10. Configure the administrative network interface.

Define the IP address, network mask, and gateway of the internal interface which is going to be the administrative network interface. The default values are:

IP Address: 192.168.2.100

Netmask: 255.255.255.0

Gateway: none

You need to change the gateway value only if you wish to use the WebAdmin interface from a workstation outside the subnet defined by the netmask.

Note that the gateway itself must be within the subnet.⁴

Confirm your settings with the **Enter** key.

11. Accept installation of the Enterprise Toolkit.

You can decide to install Open Source software only. However, we advise to also install the Enterprise Toolkit to be able to use the full functionality of Astaro Security Gateway.

Press **Enter** to install both software packages or **Esc** to install the Open Source software only.

12. Confirm the warning message to start the installation.

Please read the warning carefully. After confirming, all existing data on the PC will be destroyed.

If you want to change your settings, press **F12** to return to Step 2. Otherwise, start the installation process by pressing **F8**.

The software installation process can take up to a couple of minutes. You can follow the progress of the installation using one of the four monitoring consoles:

- Installation routine (**Alt+F1**)
- Interactive Bash console 1 (**Alt+F2**)
- Installation log (**Alt+F3**)
- Kernel log (**Alt+F4**)

13. Remove the CD-ROM, connect to the internal network, and reboot the system.

When the installation process is complete, remove the CD-ROM from the drive and connect the **eth0** network card to the internal network. Except for the internal network card (**eth0**), the sequence of network cards normally will be determined by PCI ID and by the kernel drivers. The sequence of network card names may also change if the hardware configuration is changed, especially if network cards are removed or added.

Then reboot the security system by pressing **Ctrl+Alt+Del** or the Reset button. During the boot process, the IP addresses of the internal network

⁴ For example, if you are using a network mask of 255.255.255.0, the subnet is defined by the first three octets of the address: in this case, 192.168.2. If your administration computer has the IP address 192.168.10.5, it is not on the same subnet, and thus requires a gateway. The gateway router must have an interface on the 192.168.2 subnet and must be able to contact the administration computer. In our example, assume the gateway has the IP address 192.168.2.1.

cards are changed. The installation routine console (Alt+F1) may display the message "No IP on eth0" during this time.

After Astaro Security Gateway has rebooted (a process which, depending on your hardware, can take several minutes), ping the IP address of the eth0 interface to ensure it is reachable. If no connection is possible, please check if one of the following problems is present:

- The IP address of Astaro Security Gateway is incorrect.
- The IP address of the client computer is incorrect.
- The default gateway on the client is incorrect.
- The network cable is connected to the wrong network card.
- All network cards are connected to the same hub.

Basic Configuration

The second step of the installation is performed through WebAdmin, the web-based administrative interface of Astaro Security Gateway. Prior to configuring basic system settings, you should have a plan how to integrate Astaro Security Gateway into your network. You must decide which functions you want it to provide, for example, if you want to operate it in bridge mode or in standard (routing) mode, or how you want it to control the data packets flowing between its interfaces. However, you can always reconfigure Astaro Security Gateway at a later time. So if you do not have planned how to integrate Astaro Security Gateway into your network yet, you can begin with the basic configuration right away.

1. Start your browser and open WebAdmin.

Browse to the URL of Astaro Security Gateway (i.e., the IP address of eth0). In order to stay consistent with our configuration example above, this would be <https://192.168.2.100:4444> (note the HTTPS protocol and port number 4444).

Deviating from the configuration example, each Astaro Security Gateway Appliance ships with the following default settings:

- **Interfaces:** Internal network interface (eth0)
- **IP address:** 192.168.0.1

- **Network mask:** 255.255.255.0
- **Default gateway:** none

To access WebAdmin of any Astaro Security Gateway Appliance, enter the following URL instead:

<https://192.168.0.1:4444>

To provide authentication and encrypted communication, Astaro Security Gateway comes with a self-signed security certificate. This certificate is offered to the web browser when an HTTPS-based connection to WebAdmin is established. The browser will display a security warning. Once you have accepted the certificate, the initial login page is displayed.

The screenshot shows the 'Welcome to WebAdmin' interface. At the top, it says 'Welcome to WebAdmin'. Below that, a title bar reads 'Basic system setup'. The form contains fields for 'Hostname', 'Company or Organization Name', 'City', 'Country' (with a dropdown menu showing ':: Please select ::'), 'admin account password', 'Repeat password', and 'admin account email address'. To the right of these fields is a note: 'These settings must be made before the system can be used. Please note that ALL fields must be filled in. After applying the settings, log into the system with username admin and the password you set below.' Below the form is a section titled 'IMPORTANT--READ CAREFULLY BEFORE OPERATING THIS SOFTWARE' containing a license agreement text. At the bottom, there are two buttons: 'I accept the license agreement' (unchecked) and 'Perform basic system setup' (checked).

Figure 1.2 The Initial Login Page of WebAdmin

2. Fill out the Basic System Setup form.

Enter accurate information of your company in the text boxes presented here. In addition, specify a password and valid e-mail address for the administrator account. If you accept the license agreement, click the *Perform Basic System Setup* button to continue logging in. While performing the basic system setup, a number of certificates and certificate authorities are being created:

- **WebAdmin CA:** The CA with which the WebAdmin certificate was signed (see *Management >> WebAdmin Settings >> HTTPS Certificate*).
- **VPN Signing CA:** The CA with which digital certificates are signed that are used for VPN connections (see *Site-to-site VPN >> Certificate Management >> Certificate Authority*).
- **WebAdmin Certificate:** The digital certificate of WebAdmin (see *Site-to-site VPN >> Certificate Management >> Certificates*).
- **Local X.509 Certificate:** The digital certificate of Astaro Security Gateway that is used for VPN connections (see *Site-to-site VPN >> Certificate Management >> Certificates*).

The login page appears. (With some browsers it may, however, happen that you are presented another security warning because the certificate has changed according to your entered values.)



Figure 1.3 Astaro Security Gateway Login Screen

3. Log in to WebAdmin.

Type admin in the *Username* field and enter the password you have specified on the previous screen.

A configuration wizard is presented to you which will guide you through the initial configuration process. Follow the steps to configure the basic settings of Astaro Security Gateway.

If you have a backup file, you can decide to restore this backup file instead (please refer to section *Backup Restoration*).

Alternatively, you can safely click *Cancel* (at any time during the wizard's steps) and thereby exit the wizard, for example if you want to configure Astaro Security Gateway directly in WebAdmin. You can also click *Finish* at any time to save your settings done so far and exit the wizard.

4. Install your license.

Click the folder icon to upload your purchased license (a text file). Click Next to install the license.

In case you did not purchase a license, click Next to use the built-in 30-day trial license with all features enabled that is shipped with Astaro Security Gateway.

5. Configure the internal network interface.

Check the presented settings for the internal network interface (eth0). The settings for this interface are based on the information you provided during the installation of the software. Additionally, you can set the Astaro Security Gateway to act as DHCP server on the internal interface by selecting the checkbox.

Note – If you change the IP address of the internal interface, you must connect to WebAdmin again using the new IP address after finishing the wizard.

6. Select the uplink type for the external interface.

Select the connection type of your uplink/Internet connection the external network card is going to use. The type of interface and its configuration depend on what kind of connection to the Internet you are going to use. Click Next.

In case the Astaro Security Gateway has no uplink or you do not want to configure it right now, just leave the *Internet Uplink Type* input box blank. If you configure an Internet uplink, IP masquerading will automatically be configured for connections from the internal network to the Internet.

If you select *Standard Ethernet Interface with Static IP Address*, specifying a *Default Gateway* is optional. If you leave the text box blank, your default gateway setting of the installation routine will persist.

You can skip each of the following steps by clicking *Next*. You can make and change those skipped settings later in WebAdmin.

7. Make your basic firewall settings.

You can now select what types of services you want to allow on the Internet. Click Next to confirm your settings.

8. Make your basic intrusion prevention settings.

You can now make settings regarding intrusion prevention for several operation systems and databases. Click Next to confirm your settings.

9. Make your settings for Instant Messaging and P2P.

You can now select which Instant Messaging or Peer-to-Peer protocols should be blocked. Click Next to confirm your settings.

10. Make your Web Security settings.

You can now select whether the web traffic should be scanned for viruses and spyware. Additionally, you can select to block web pages that belong to certain categories. Click Next to confirm your settings.

11. Make your Mail Security settings.

You can now select the first checkbox to enable the POP3 proxy. You can also select the second checkbox to enable the ASG as inbound SMTP relay: Enter the IP address of your internal mail server and add SMTP domains to route. Click Next to confirm your settings.

12. Confirm your settings.

A summary of your settings is displayed. Click *Finish* to confirm them or *Back* to change them. However, you can also change them in WebAdmin later.

After clicking *Finish* your settings are saved and you are redirected to the Dashboard of WebAdmin, providing you with the most important system status information of the Astaro Security Gateway unit.



Figure 1.4 System Dashboard of Astaro Security Gateway

If you encounter any problems while completing these steps, please contact the support department of your Astaro Security Gateway supplier. For more information, you might also want to visit the following websites:

- Astaro Bulletin Board⁵
- Astaro Knowledgebase⁶

Backup Restoration

The WebAdmin configuration wizard (see Basic Configuration) allows you to restore an existing backup file instead of going through the basic configuration process. Do the following:

1. Select Restore existing backup file in the configuration wizard.

Select *Restore existing backup file* in the configuration wizard and click *Next*.

You are directed to the upload page.

2. Upload the backup.

Click the folder icon, select the backup file you want to restore, and click *Start Upload*.

3. Restore the backup.

Click *Finish* to restore the backup.

Important note – You will not be able to use the configuration wizard afterwards.

As soon as the backup has been restored successfully you will be redirected to the login screen.

⁵ <http://www.astaro.org/>

⁶ <http://www.astaro.com/kb/>

Chapter 2

WebAdmin

WebAdmin is the web-based administrative interface that allows you to configure every aspect of Astaro Security Gateway. WebAdmin consists of a menu and pages, many of which have multiple tabs. The menu on the left of the screen organizes the features of Astaro Security Gateway in a logical manner. When you select a menu item, such as *Network*, it expands to reveal a submenu and the associated page opens. Note that for some menu items no page is associated. Then, the page of the previously selected menu or submenu item keeps being displayed. You have to select one of the submenu items, which opens the associated page at its first tab.

The procedures in this administration guide direct you to a page by specifying the menu item, submenu item, and the tab, for example: "On the *Network >> Interfaces >> Hardware* tab, configure ..."

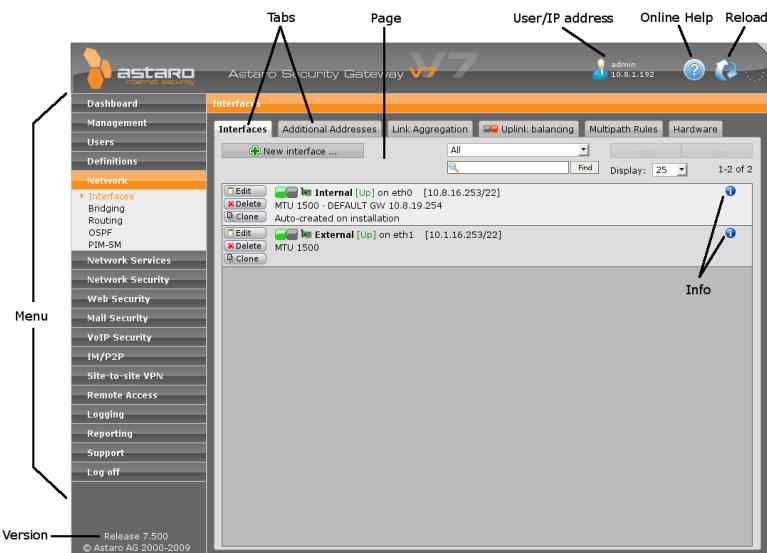


Figure 2.1 WebAdmin

WebAdmin Menu

The WebAdmin menu provides access to all configuration options of Astaro Security Gateway, that is, there is no need for using a command line interface to configure specific parameters.

- **Dashboard:** The Dashboard graphically displays a snapshot of the current operating status of the Astaro Security Gateway unit.
- **Management:** Configure basic system and WebAdmin settings as well as all settings that concern the configuration of the Astaro Security Gateway unit.
- **Users:** Configure user accounts, user groups, and external authentication servers for use with the Astaro Security Gateway unit.
- **Definitions:** Configure network, service, and time event definitions used throughout the Astaro Security Gateway unit.
- **Network:** Configure system facilities such as network interfaces as well as routing options, among other things.
- **Network Services:** Configure network services such as DNS and DHCP, among other things.
- **Network Security:** Configure basic network security features such as packet filter rules or intrusion prevention settings.
- **Web Security:** Configure the HTTP/S and FTP proxies of the Astaro Security Gateway unit.
- **Mail Security:** Configure the SMTP and POP3 proxies of the Astaro Security Gateway unit as well as e-mail encryption.
- **VoIP Security:** Configure control of VoIP traffic passing the firewall.
- **IM/P2P Security:** Configure control of Instant Messaging and Peer-to-Peer traffic passing the firewall.
- **Site-to-site VPN:** Configure site-to-site Virtual Private Networks.
- **Remote Access:** Configure remote access VPN connections to the Astaro Security Gateway unit.
- **Logging:** Configure logging settings and view log messages.

- **Reporting:** View overview statistics about the utilization of the Astaro Security Gateway unit.
- **Support:** Access to the support tools available at the Astaro Security Gateway unit.
- **Log Off:** Log out of the user interface.

Button Bar

The buttons in the upper right corner of WebAdmin provide access to the following features:

- **User/IP Address:** Shows the currently logged in user and the IP address from which WebAdmin is accessed.
- **Online Help:** Every menu, submenu, and tab has an online help screen that provides context-sensitive information and procedures related to the controls of the current WebAdmin page.

Note – The online help is updated by means of pattern updates and always describes the most recent version of Astaro Security Gateway, which might cause minor inconsistencies between the online help and the currently installed firmware.

- **Reload:** To request the already displayed WebAdmin page again, always click the *Reload* button.

Note – Never use the reload button of the browser, because otherwise you will be logged out of WebAdmin.

Lists

Many pages in WebAdmin consist of lists. The buttons on the left of each list item enable you to edit or delete the item. To add an item to the list, click the *New ...* button, where "..." is a placeholder for the object being created (e.g., Interface). This opens a dialog box where you can define the properties of the new object.

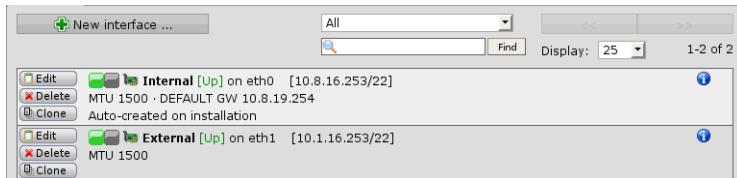


Figure 2.2 Example of a WebAdmin List

Each list lets you sort all items according to their type. In addition, the search box lets you search for items specifically. Enter a search string and click *Find*.

Note that lists with more than ten items are split into several chunks, which can be browsed with Next (>>) and Previous (<<) buttons.

Tip – Clicking on the info icon will show all configuration options in which the object is used.

Dialog Boxes

Dialog boxes are special windows which are used by WebAdmin to prompt you for entering specific information. The example shows a dialog box for creating a new static route in the *Network >> Static Routing* menu.

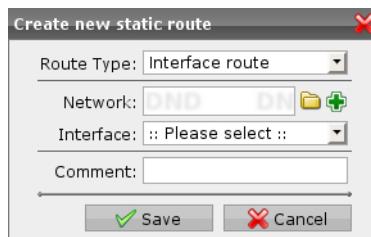


Figure 2.3 Example of a WebAdmin Dialog Box

Each dialog box can consist of various widgets such as text boxes, checkboxes, and so on. In addition, many dialog boxes offer a drag-and-drop functionality, which is indicated by a special background reading *DND*. Whenever you encounter such a box, you can drag an object into the box. To open the window from where to drag the objects, click the folder icon that is located right next to the text box. Depending on the configuration option, this opens the list of available network, service, or time event definitions. Clicking the green plus

icon opens a second dialog box letting you create a new definition. Some widgets that are not necessary for a certain configuration are grayed out. In some cases, however, they can still be edited, but having no effect.

Note – You may have noticed the presence of both *Save* and *Apply* buttons in WebAdmin. The *Save* button is used in the context of creating or editing objects in WebAdmin such as static routes or network definitions. It is always accompanied by a *Cancel* button. The *Apply* button, on the other hand, serves to confirm your settings in the backend, thus promptly activating them.

Buttons and Icons

WebAdmin has some buttons and functional icons whose usage is described here.

Buttons

-  **View** Shows a dialog window with detailed information on the object.
-  **Edit** Opens a dialog window to edit properties of the object.
-  **Delete** Deletes the object. If an object is still in use somewhere, there will be a warning. Not all objects can be deleted if they are in use.
-  **Clone** Opens a dialog window for creating an object with identical settings/properties. Helps you to create similar objects without having to type all identical settings over and over again.

Functional Icons

-  **Info:** Shows all configurations where the object is in use.
-  **Status:** Enables or disables a function. Green when enabled, red when disabled, and amber when configuration is required before enabling.
-  **Folder:** Has two different functions: (1) Opens a group tooltip (see section below) on the left side where you can choose appropriate objects from. (2) Opens a dialog window to upload a file.
-  **Plus:** Opens a dialog box to add a new object of the required type.
-  **Recycle Bin:** Removes an object from the current configuration. The object is however not deleted.
-  **Import:** Opens a dialog window to import text with more than one item or line. Enhances adding multiple items without having to type them individually, e.g. a large blacklist to the URL blacklist. Copy the text from anywhere and enter it using CTRL+V.
-  **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.
-  **Sort:** By using the two arrows, you can sort list elements by moving an element down or up, respectively.
-  **PDF:** Saves the current view of data in a PDF file and then opens a dialog window to download the created file.
-  **CSV:** Saves the current view of data in a CSV (comma-separated values) file and then opens a dialog window to download the created file.

Group Tooltips

A group tooltip is a drag-and-drop object list which is sometimes displayed on the left side of WebAdmin, covering the main menu temporarily.

It is opened automatically when you click on the folder icon (see section above), or you can open it manually via a keyboard shortcut (see *Management >> WebAdmin Settings >> User Preferences*).

The *Group Tooltips* give you quick access to WebAdmin objects like users/groups, interfaces, networks, and services to be able to select them for configuration purposes. Objects are selected simply by dragging and dropping them onto the current configuration.

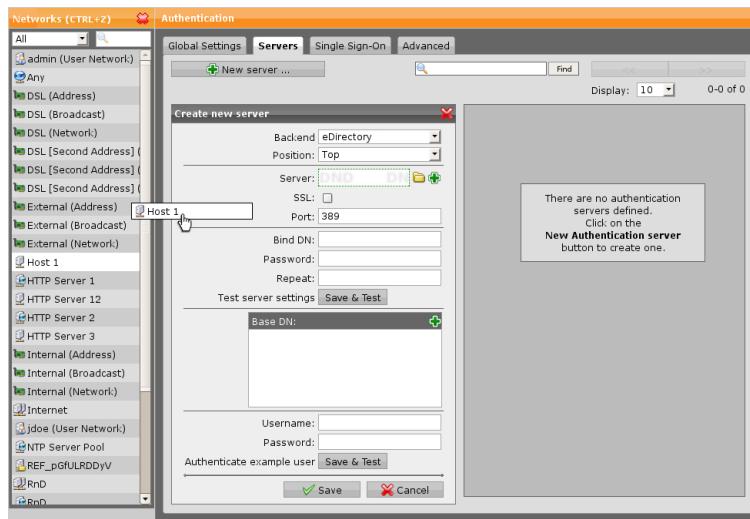


Figure 2.4 Dragging an Object From the Group Tooltip Networks

According to the different existing object types, there are five different types of group tooltips. Clicking the folder icon will always open the type required by the current configuration.

Chapter 3

Dashboard

The Dashboard graphically displays a snapshot of the current operating status of Astaro Security Gateway. By default, the Dashboard is updated at intervals of five seconds. You can configure the refresh rate from Never to 60 seconds.

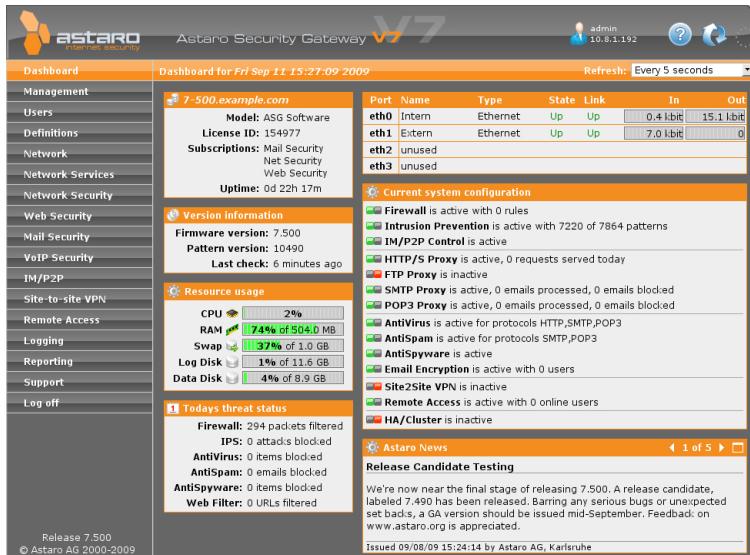


Figure 3.1 Example ASG Software V7 WebAdmin Dashboard

The Dashboard displays by default when you log in to WebAdmin and shows the following information:

- General Information:** Hostname, model, license ID, and uptime of the unit.
- Version Information:** Information on the currently installed firmware and pattern versions as well as available updates.
- Resource Usage:** Current system utilization, including the following components:

- The CPU utilization in percent
 - The RAM utilization in percent
 - The swap utilization in percent
 - The amount of hard disk space consumed by the log partition in percent
 - The amount of hard disk space consumed by the root partition in percent
 - The status of the UPS (uninterruptible power supply) module (if available)
- **Today's Threat Status:** A counter for the most relevant security threats detected since midnight:
 - The total of dropped and rejected data packets for which logging is enabled
 - The total of blocked intrusions attempts
 - The total of blocked viruses (all proxies)
 - The total of blocked spam messages (SMTP/POP3)
 - The total of blocked spyware (all proxies)
 - The total of blocked URLs (HTTP/S)
 - **Interfaces:** Name and status of configured network interface cards. In addition, information on the average bitrate of the last 75 seconds for both incoming and outgoing traffic is shown. The values presented are obtained from bitrate averages based on samples that were taken at intervals of 15 seconds. Clicking the traffic icons of an interface opens a traffic monitor. For more information please see *Network Security >> Packet Filter >> Advanced*.
 - **Current System Configuration:** Enabled/disabled representation of the most relevant security features:
 - **Firewall:** Packet filtering including information about the total of active rules.
 - **Intrusion Prevention:** The intrusion prevention system (IPS) recognizes attacks by means of a signature-based IPS ruleset.

- **HTTP Proxy:** An application-level gateway for the HTTP/S protocol, featuring a rich set of web filtering techniques for the networks that are allowed to use its services.
- **FTP Proxy:** An application-level gateway for file transfers via the *File Transfer Protocol* (FTP).
- **SMTP Proxy:** An application-level gateway for messages sent via the *Simple Mail Transfer Protocol* (SMTP).
- **POP3 Proxy:** An application-level gateway for messages sent via the *Post Office Protocol 3* (POP3).
- **AntiVirus:** Protection of your network from web traffic that carries harmful and dangerous content such as viruses, worms, or other malware.
- **AntiSpam:** Detection of unsolicited spam e-mails and identification of spam transmissions from known or suspected spam purveyors.
- **AntiSpyware:** Protection from spyware infections by means of two different virus scanning engines with constantly updated signature databases and spyware filtering techniques that protects both inbound and outbound traffic.
- **E-mail Encryption:** Encryption, decryption, and digitally signing of e-mails using the S/MIME or OpenPGP standard.
- **Site2site VPN:** Configuration of site-to-site VPN scenarios.
- **Remote Access:** Configuration of roadwarrior VPN scenarios.
- **HA/Cluster:** High-availability (HA) failover and clustering, that is, the distribution of processing-intensive tasks such as content filtering, virus scanning, intrusion detection, or decryption equally among multiple cluster nodes.

Management

This chapter describes how to configure basic system settings as well as the settings of the web-based administrative interface of Astaro Security Gateway, *WebAdmin*, among others. The *Overview* page shows statistics of the last login attempts to WebAdmin.

The following topics are included in this chapter:

- System Settings
- WebAdmin Settings
- Licensing
- Up2Date
- Backup/Restore
- User Portal
- Notifications
- Customization
- SNMP
- Central Management
- High-Availability
- Shutdown/Restart

System Settings

The tabs under *System Settings* allow you to configure basic settings of your firewall such as hostname, date, and time.

Organizational

Enter the name and location of your organization and an e-mail address to reach the person or group technically responsible for the operation of your Astaro Security Gateway. Note that this data is also used in certificates for IPSec, e-mail encryption and WebAdmin.

Hostname

Enter the hostname of your firewall in the form of a *fully qualified domain name* (FQDN) into this field, for example ASG.example.com. A hostname may contain alphanumeric characters, dots, and hyphens. At the end of the hostname there must be a special designator such as com, org, or de. The hostname will be used in notification messages to identify the firewall. It will also appear in status messages sent by the HTTP/S proxy. Note that the hostname does not need to be registered in the DNS zone for your domain.

Time and Date

You can set your firewall's date, time, and time zone so that the date and time appear correctly in the firewall logs. Alternatively, you can have them set automatically using a network time server. Note that the NTP server synchronization takes place hourly. In addition, significant changes in the time settings will appear as gaps in logging and reporting data.

If you operate multiple interconnected firewalls that span several time zones, select the same time zone for all devices, for example UTC (Coordinated Universal Time)—this will make log messages much easier to compare.

Note that when the system time is changed, you may encounter undesired side-effects:

- **Turning the clock forward**

For example, when changing standard time to daylight saving time.

- The timeout period of WebAdmin will expire and the session is no longer valid.
- Time-based reports will contain no data for the skipped hour. In most graphs, this time span will appear as a straight line in the amount of the latest recorded value.
- Accounting reports will contain values of 0 for all variables during this time.

- **Turning the clock back**

For example, when changing daylight saving time to standard time.

- There is already log data for the corresponding time span in time-based reports.
- Most diagrams will display the values recorded during this period as compressed.
- The elapsed time since the last pattern check (as displayed on the Dashboard) shows the value "never", even though the last check was in fact only a few minutes ago.
- Automatically created certificates on the security system may become invalid because the beginning of their validity periods would be in the future.
- Accounting reports will retain the values recorded from the future time. Once the time of the reset is reached again, the accounting data will be written again as normal.

Because of these drawbacks the system time should only be set once when setting up the system with only small adjustments being made thereafter. This especially holds true if accounting and reporting data needs to be processed further and accuracy of the data is important.

Set Time And Date

To configure the system time manually select date and time from the respective drop-down lists. Click *Apply* to save your settings.

Set Timezone

To change the system's timezone, select an area or a timezone from the drop-down list. Click *Apply* to save your settings.

Synchronize Time With Internet Server

To synchronize the system time using a timeserver, select one or more NTP

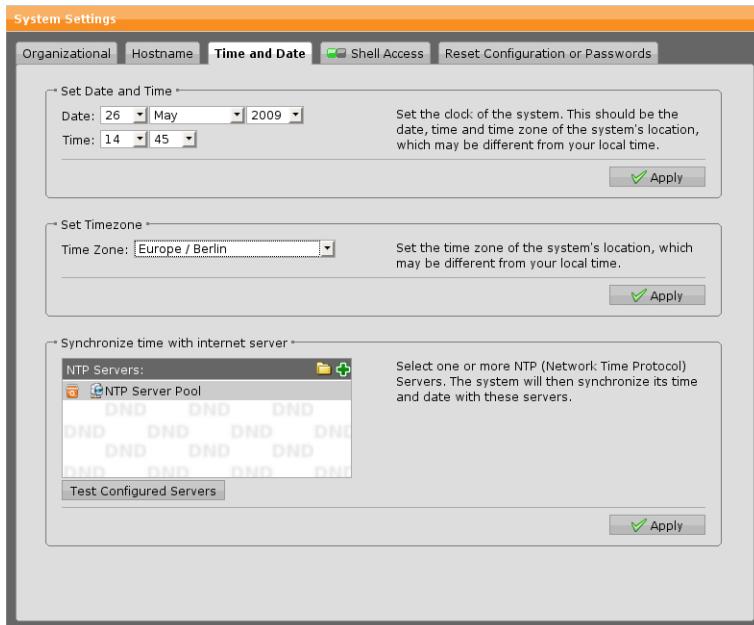


Figure 4.1 Configuring Time and Date

servers. Click *Apply* after you have finished the configuration to save your changes.

NTP Server: The *NTP Server Pool* is selected by default. This network definition is linked to the big virtual cluster of timeservers of the *pool.ntp.org* project. Alternatively, you can either select other NTP server definitions or create new ones.

Adding more timeservers will make it less likely that your system time can be influenced by a malfunctioning NTP server, for a slight increase in resource usage.

Test Configured Servers: Click this button if you want to test whether a connection to the selected NTP server(s) can be established from your device and whether it returns usable time data. This will measure the time offset between your system and the servers. Offsets should generally be well below one second if your system is configured correctly. As test result, you will be displayed an information on the connection status.

Shell Access

Secure Shell (SSH) is a command-line access mode primarily used to gain remote shell access to the firewall. It is typically used for low-level maintenance or troubleshooting. To access this shell you need an SSH client, which usually comes with most Linux distributions.

Allowed Networks: Use the *Allowed Networks* control to restrict access to this feature to certain networks only. Networks listed here will be able to connect to the SSH service.

Shell User Passwords: Enter passwords for the default shell accounts `root` and `loginuser`. To change the password for one out of these two accounts only, just leave both input boxes for the other account blank.

Note – To enable SSH shell access, passwords must be set initially. In addition, you can only specify passwords that adhere to the password complexity settings as configured on the *Users >> Authentication >> Advanced* tab. That is, if you have enabled complex passwords, shell user passwords must meet the same requirements.

SSH Daemon Listen Port: This option lets you change the TCP port used for SSH. By default, this is the standard SSH port 22. To change the port, enter an appropriate value in the range from 1024 to 65535 in the *Port Number* box and click *Apply*.

Reset Configuration or Passwords

The options on the *Reset Configuration or Passwords* tab let you delete the passwords of the shell users. In addition, you can execute a factory reset.

Reset System Passwords: Executing this function will reset the passwords of the following users:

- `root` (shell user)
- `loginuser` (shell user)
- `admin` (predefined administrator account)

In addition, to halt the system, select the *Shutdown System Afterwards* option.

Security Note – The next person connecting to the Webadmin will be presented an *Admin Password Setup* dialog window. Thus, after resetting the passwords,

you should usually quickly log out, reload the page in your browser, and set a new admin password.

Besides, shell access will not be possible any more until you set new shell passwords on the *Management >> System Settings >> Shell Access* tab.

Factory Reset: This function resets the device back to the factory default configuration. The following data will be deleted:

- System configuration
- HTTP/S proxy cache
- Logs and accounting data
- Databases
- Update packages
- Licenses
- Passwords
- High-availability status

However, the version number of Astaro Security Gateway Software will remain the same, that is, all firmware and pattern updates that have been installed will be retained.

Note – Astaro Security Gateway will shut down once a factory reset has been initiated.

WebAdmin Settings

The tabs under *Management >> WebAdmin Settings* allow you to configure basic WebAdmin settings such as the TCP port and language, among other things.

General

WebAdmin Language

Select the language of WebAdmin. Note that this applies to the current user profile only.

WebAdmin Idle Timeout

In the *Log Out After* box you can specify the period of time (in seconds) how long a WebAdmin session can remain idle before the administrator is forced to log in again. By default, the idle timeout is set to 300 seconds. The range is from 60 to 86,400 seconds.

Note – For a new timeout value to take effect you have to log in to WebAdmin again. Note that when you have opened the *Dashboard* page of WebAdmin, the auto logout function is disabled.

WebAdmin TCP Port

By default, port (4444) is used as WebAdmin TCP port. In the *TCP Port* box you can enter either 443 or any value between 1024 and 65535. However, certain ports are reserved for other services. In particular, you can never use port 10443, and you cannot use the same port you are using for the User Portal or for SSL remote access. Note that you must add the port number to the IP address (separated by a colon) in the browser's address bar when accessing WebAdmin, for example <https://192.168.0.1:1443>. Click *Apply* to save your settings.

Access Control

Allowed Administrators: Astaro Security Gateway can be administered by multiple administrators simultaneously. In the *Allowed Administrators* box you can specify which users or groups should have unlimited read and write access to the WebAdmin interface. By default, this is the group of *SuperAdmins*.

Allowed Auditors: Astaro Security Gateway also offers limited login access for auditors, who are only allowed to read log files and reporting information but cannot change any settings. In the *Allowed Auditors* box you can specify which users or groups should have access to the WebAdmin interface with these limited permissions. By default, this box is empty.

Allowed Networks: The *Allowed Networks* box lets you define the networks that should be able to connect to the WebAdmin interface. For the sake of a smooth installation of the firewall, the default is Any. This means that the WebAdmin interface can be accessed from everywhere. Change this setting to your internal network(s) as soon as possible. The most secure solution, however, would be to limit the access to the firewall to only one administrator PC through HTTPS.

Allowed Reviewers: Users and groups with reviewer rights are allowed to see everything in WebAdmin but are not allowed to change or create anything. In

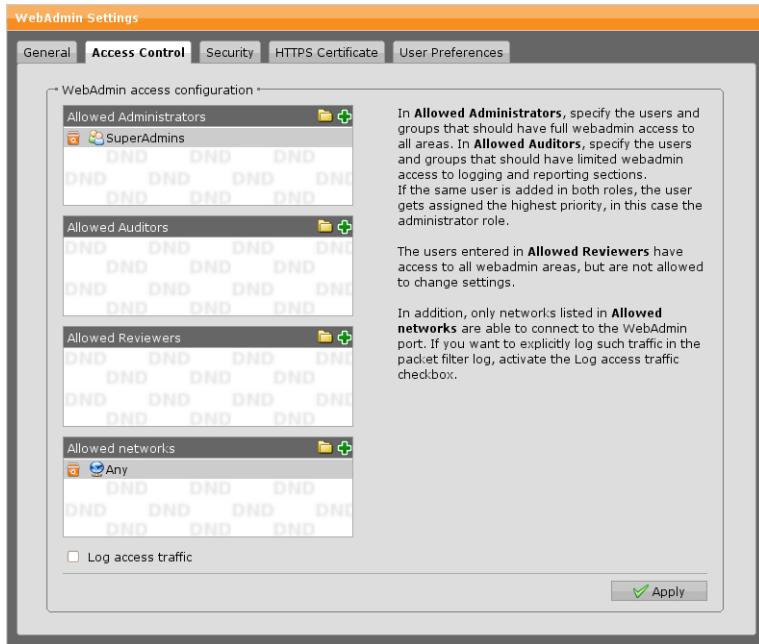


Figure 4.2 Configuring Access Control

the *Allowed Reviewers* box you can specify which users or groups should have access to the WebAdmin interface with these limited permissions. By default, this box is empty.

Log Access Traffic: If you want to log all WebAdmin access activities in the packet filter log, select the *Log Access Traffic* checkbox.

Security

Block Password Guessing: This function can be used to prevent password guessing. After a configurable number of failed login attempts (default: 3), the IP address trying to gain WebAdmin access will be blocked for a configurable amount of time (default: 600 seconds). Networks listed in the *Never Block Networks* box are exempt from this check.

HTTPS Certificate

On the *Management >> WebAdmin Settings >> HTTPS Certificate* tab you can import the WebAdmin CA certificate into your browser.

During the initial setup of the WebAdmin access you have automatically created a local CA certificate on the firewall. The public key of this CA certificate can be installed into your browser to get rid of the security warnings when accessing the WebAdmin interface.

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

To import the CA certificate, proceed as follows:

1. **On the *HTTPS Certificate* tab, click *Import CA Certificate*.**
The public key of the CA certificate will be exported.
You can either save it to disk or install it into your browser.
 2. **Install the certificate (optional).**
The browser will open a dialog box letting you choose to install the certificate immediately.
-

Note – Due to different system times and time zones the certificate might not be valid directly after its creation. In this case, most browsers will report that the certificate has expired, which is not correct. However, the certificate will automatically become valid after a maximum of 24 hours and will stay valid for 27 years.

Re-generate WebAdmin Certificate

The WebAdmin certificate refers to the hostname you have specified during the initial login. If the hostname has been changed in the meantime, the browser will display a warning message. To avoid this, you can create a certificate taking the new hostname into account. For that purpose, enter the hostname as desired and click *Apply*. Note that due to the certificate change, to be able to continue working in WebAdmin, you probably need to reload the page via your web browser, accept the new certificate, and log back into WebAdmin.

User Preferences

On the *Management >> WebAdmin Settings >> User Preferences* tab you can configure some user preferences such as global shortcuts and items per page for the currently logged in user.

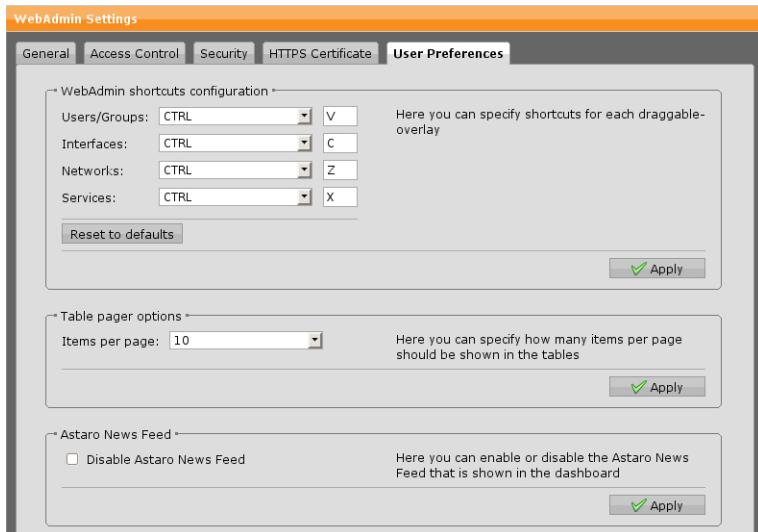


Figure 4.3 Configuring User Preferences

WebAdmin Shortcuts Configuration

Here you can configure shortcuts to switch between group tooltips, the drag-and-drop object lists used in many configurations (for more information see *WebAdmin >> Group Tooltips*). This feature allows you to see the group tooltips without having to edit anything first. Use the drop-down field to select a different modifier key and the text box to enter a different character.

If you want to return to the default settings, click the *Reset to Defaults* button. Click *Apply* to save your changes.

Table Pager Options

Here you can globally define the pagination of tables for WebAdmin, i.e. how many items are displayed per page. Click the drop-down list and select a value. Click *Apply* to save your changes.

Astaro News Feed

Astaro News Feed, if enabled, is a small section on the Dashboard where news about Astaro and its products are announced. It is disabled by default. To enable it, unselect the checkbox *Disable Astaro News Feed* and click *Apply*.

Licensing

The availability of certain features on Astaro Security Gateway, Astaro Mail Gateway, and Astaro Web Gateway is defined by licenses and subscriptions, i.e. the licenses and subscriptions you have purchased with your firewall or gateway enable you to use certain features and others not.

Starting in October 2009, Astaro introduces a new licensing model called *On-Demand Licensing* which is going to bit by bit replace the *Classic Licensing*. Classic licenses you have already purchased will, however, stay valid!

How to obtain a license

Once you have received the activation keys by e-mail after purchasing an Astaro license, you must use these keys in order to create your license or upgrade an existing license. To activate a license, you have to log in to the Astaro Partner Portal and visit the license management page. At the top of the page is a form where you can cut and paste the activation key from the e-mail into this field.

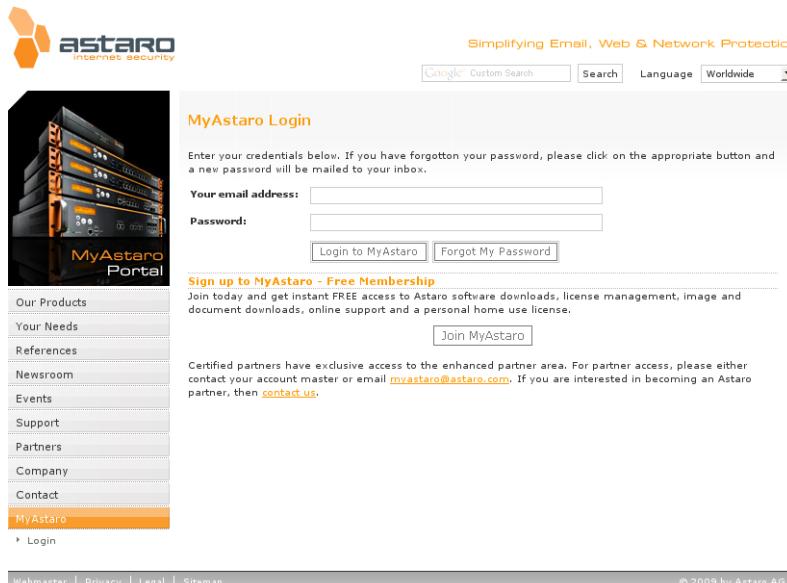


Figure 4.4 MyAstaro Portal

Another form appears asking you to fill in information about the reseller you purchased the license from as well as your own details. Astaro tries to pre-fill as much of this form as possible. Also, Astaro collects the ASG hardware serial number on this form if appropriate. After submitting this form, your license

is created, and you are forwarded to the license detail page to download the license file.

To actually use the license, you must download the license file to your hard drive and then log in to your WebAdmin installation. In WebAdmin, navigate to the *Management >> Licensing >> Installation* tab and use the upload function to find the license text file on your hard drive. Upload the license file, and WebAdmin will process it to activate any subscriptions and other settings that the license outlines.

Note – The activation key you received by e-mail cannot be imported into WebAdmin. This key is only used to activate the license. Only the license file can be imported to the security system.

OnDemand Licensing

Astaro's OnDemand licensing model is easier and much more flexible than the classic licensing model.

First, there is a base license, similar to the free home user license of the classic licensing model, providing basic functionalities for free—and not anymore for home users only but also for business users.

Second, there are three kinds of purchase subscriptions:

- Net Security
- Web Security
- Mail Security

Those can be purchased separately or in combination. Each of the subscriptions enables certain features of the product. The table below gives you an overview which features are enabled with which subscription.

For more detailed information on subscriptions and their feature set please refer to your certified Astaro Partner or the Astaro homepage⁷.

Up2Dates

Each subscription enables full automatic update support, i.e. you will be automatically informed about new firmware updates. Also, firmware and pattern updates can be downloaded (and installed) automatically.

⁷ <http://www.astaro.com/>

Feature	Base License	Net	Web	Mail
Management (Backup, Notifications, SNMP, ACC, ...)	✓			
Local Authentication (Users, Groups)	✓			
Basic Networking (Static Routing, DHCP, DNS, Auto QoS, NTP, ...)	✓			
Firewall/NAT (Packet Filter, DNAT, SNAT, ...)	✓			
PPTP & L2TP Remote Access	✓			
Local Logging, standard executive reports	✓			
Intrusion Prevention (Patterns, DoS, Flood, Portscan ...)		✓		
IPSec & SSL Site-to-site VPN, IPSec & SSL Remote Access		✓		
Advanced Networking (Link Aggregation, link balancing, Policy Routing, OSPF, Multicast, custom QoS, Server Load Balancing, Generic Proxy ...)		✓	(✓)	(✓)
User Portal		✓	✓	✓
High Availability		✓	✓	✓
Remote Auth (AD, eDir, RADIUS, ...)		✓	✓	✓
Remote Logging, advanced executive reports (archiving, configuration)		✓	✓	✓
Basic HTTP/S & FTP Proxy			✓	
HTTP/S & FTP malware filtering			✓	
Basic SMTP Proxy, Quarantine Report, Mail Manager				✓
SMTP & POP3 malware filtering				✓

Table 4.1 Licensing: Subscriptions and Features

A base license without any subscriptions supports only limited automatic updates: solely pattern updates such as online help updates and the like will continue to be downloaded and installed automatically. You will, however, not be informed about available firmware updates, and the firmware updates have to be downloaded manually. Announcements for new firmware updates can be found in Astaro's Up2Date Blog⁸.

Support and Maintenance

The base license comes with *Web Support*. You can use Astaro's support forum⁹ and Astaro's knowledgebase¹⁰.

As soon as you purchase one of the three subscriptions you will be automatically upgraded to *Standard Support*, where you can additionally open a support case in MyAstaro Portal¹¹ or contact your certified Astaro Partner.

There is also the possibility to purchase a *Premium Support* subscription, which offers 24/7 support with an Astaro Engineer being your contact person.

Classic Licensing

The classic licensing model is going to be replaced by the OnDemand licensing model described above. Classic licensing is explained here for compatibility reasons and because it is not going to be disabled overnight but to be replaced merely bit by bit.

Astaro Security Gateway ships with a 30-day trial license with all features enabled. After expiration, you must install a valid license to further operate Astaro Security Gateway. All licenses (including free home user licenses) are created in the MyAstaro Portal¹².

Subscriptions

Astaro's Web Filtering functionality, available through an optional subscription package for Astaro Security Gateway, provides content filtering, antivirus, and spyware protection for HTTP/S as well as antivirus capabilities and file extension scanning for FTP.

If the Web Filtering subscription is not available, the following tabs in WebAdmin are disabled:

- *Web Security >> HTTP/S >> AntiVirus/Malware*
- *Web Security >> HTTP/S >> URL Filtering*
- *Web Security >> HTTP/S >> URL Filtering Categories*
- *Web Security >> HTTP/S Profiles >> Filter Actions*
- *Web Security >> FTP >> AntiVirus*

⁸ <http://up2date.astaro.com/>

⁹ <http://www.astaro.org>

¹⁰ <http://www.astaro.com/kb>

¹¹ <http://my.astaro.com>

¹² <http://my.astaro.com>

Astaro's Mail Security functionality is available through two separate subscriptions for Astaro Security Gateway solutions: Mail Filtering and Mail Encryption. Mail Filtering provides antispam, antivirus, and phishing protection. Mail Encryption, on the other hand, provides OpenPGP and S/MIME encryption and digital signatures for SMTP e-mails.

If the Mail Filtering subscription is not available, the following tabs in WebAdmin are disabled:

- *Mail Security >> SMTP >> AntiVirus*
- *Mail Security >> SMTP >> AntiSpam*
- *Mail Security >> POP3 >> AntiVirus*
- *Mail Security >> POP3 >> AntiSpam*
- All tabs of the *Mail Security >> Encryption* menu

Note – Customers, who in the past purchased either the Mail Filtering or the Mail Encryption subscription, benefit from the subscription merging in that they now can use the features of both subscriptions.

In addition, the following functions are disabled:

- *Mail Security >> SMTP >> Relaying >> Content Scan*
- *Mail Security >> SMTP >> Advanced >> BATV Secret*
- *Mail Security >> SMTP >> Advanced >> Max Message Size*
- *Mail Security >> SMTP Profiles*

To indicate that the current license does not cover a subscription feature, a warning message is displayed above the tab.

Overview

The Overview tab provides detailed information about your license and is divided into several areas:

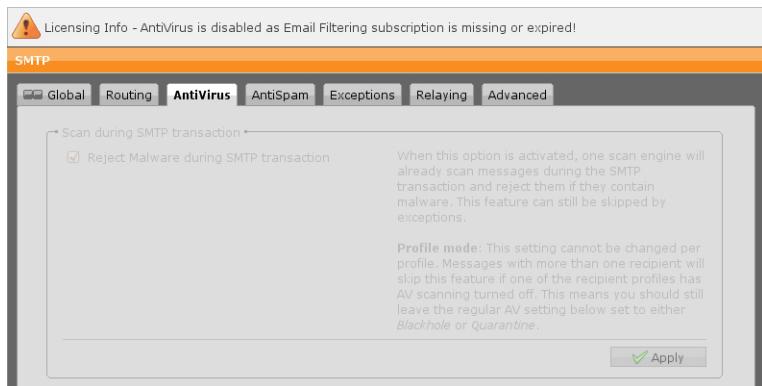


Figure 4.5 Licensing Warning Message

- **License Information:** Shows basic license parameters such as owner, ID, or expiration date.
- **Maintenance:** Shows the support level plus the date until it is valid.
- **Subscriptions:** Shows the subscriptions you have purchased with your As-taro Security Gateway unit.
- **Hot Standby/Cluster:** Shows license options for the high-availability and cluster function.

Installation

On the *Management >> Licensing >> Installation* tab you can upload and install a new license.

To install a license, proceed as follows:

1. **Open the *Upload File* dialog box.**
Click the folder icon next to the *License File* box.
The *Upload File* dialog box opens.
2. **Select the license file.**
Browse to the directory where your license file resides.
Select the license file you want to upload.
3. **Click *Start Upload*.**
Your license file will be uploaded.
4. **Click *Apply*.**
Your license will be installed. Note that the new license will automatically

Licenses

License information

- Owner:** Astaro
- License ID:** 106556
- Registration Date:** 27 November 2006
- Expiration Date:** Never
- Maximum concurrent connections:** 128000
- Maximum users:** 50
- Warranty period end date:** 25 February 2007 (expired)

Maintenance

- Level:** None » Silver » **Gold** » Platinum » Platinum Plus
- Start Date:** 27 November 2006
- End Date:** 27 November 2009

Subscriptions

- Web Filtering:** ✓ Licensed until 27 November 2009
- IM/P2P Filtering:** ✓ Licensed until 27 November 2009
- Email Filtering:** ✓ Licensed until 27 November 2009
- Email Encryption:** ✓ Licensed until 27 November 2009

Hot-Standby / Cluster

- Hot-Standby:** ✓ Enabled
- Cluster:** ✘ Not licensed

How to buy or extend a license

In order to purchase Astaro Licenses, Upgrades or renewals please contact your Certified Astaro Reseller. He will help you decide what you need and will make you a quote. If you do not have a reseller yet, please click: [here](#).

Figure 4.6 Licensing Overview (Classic Licensing)

Management » Licensing

Installation

License file upload

License file:

Please upload your license file here. The license will automatically replace any other installed license.

Figure 4.7 Installing a License

replace any other license already installed.

The installation of the license will take approximately 60 seconds.

Active IP Addresses

If you do not have a license allowing unlimited users (IP addresses), this tab displays information on IP addresses covered by your license. IP addresses that

exceed the scope of your license are listed separately. If the limit is exceeded you will receive an e-mail notification at regular intervals.

Note – IP addresses not seen for a period of seven days will automatically be removed from the license counter.

Up2Date

On the tabs of the *Management >> Up2Date* menu the configuration options for the update service of Astaro Security Gateway are located. Regularly installed updates keep your firewall up-to-date with the latest bugfixes, product improvements, and virus patterns. Each update is digitally signed by Astaro—any unsigned or forged update will be rejected.

There are two types of updates available:

- **Firmware updates:** A firmware update contains bugfixes and feature enhancements for Astaro Security Gateway Software.
- **Pattern updates:** A pattern update keeps the antivirus, antispam, intrusion prevention definitions as well as the online help up-to-date.

In order to download Up2Date packages, the firewall opens a TCP connection to the update servers on port 443—allowing this connection without any adjustment to be made by the administrator. However, if there is another firewall inbetween, you must explicitly allow the communication via the port 443 TCP to the update servers.

Overview

The *Management >> Up2Date >> Overview* tab provides a quick overview whether your system is up-to-date. From here, you can install new firmware and pattern updates.

Up2Date Progress

This section is only visible when you have triggered an installation process. Click the button *Watch Up2Date Progress in New Window* to monitor the update progress. If your browser does not suppress pop-up windows, a new window showing the update progress will be opened. Otherwise you will have to explicitly allow the pop-up window.

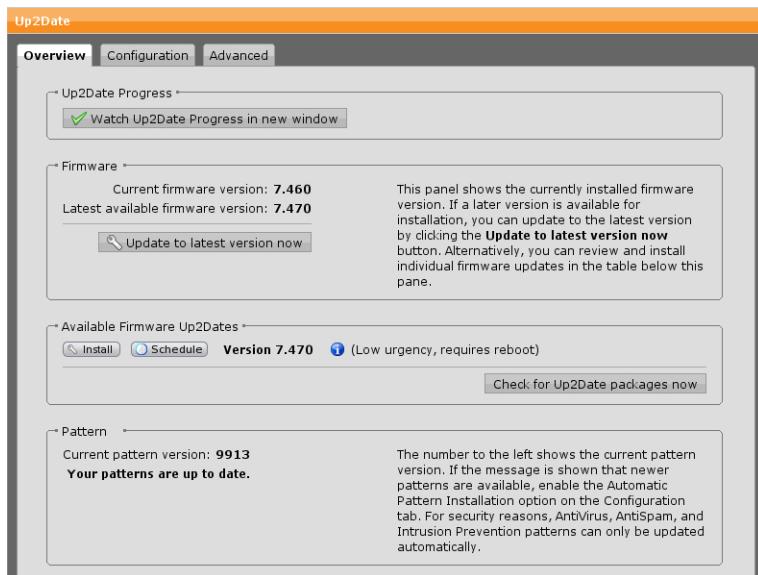


Figure 4.8 Up2Date Overview page

Note – A backup will be sent to the standard backup e-mail recipients before an installation process is started.

Firmware

The **Firmware** section shows the currently installed firmware version. If an update package is available, a button *Update to Latest Version Now* is displayed. Additionally, you will see a message in the *Available Firmware Up2Dates* section. You can directly download and install the most recent update from here. Once you have clicked *Update To Latest Version Now*, you can watch the update progress in new a window. For this, click the *Reload* button of WebAdmin.

Available Firmware Up2Dates

If you have selected *Manual* on the *Configuration* tab, you can see a *Check for Up2Date Packages Now* button in this section, which you can use to download firmware Up2Date packages manually. If there are more than one Up2Dates available, you can select which one you are going to install. You can use the *Update to Latest Version Now* in the *Firmware* section if you want to install the most recent version directly.

There is a *Schedule* button available for each Up2Date with which you can

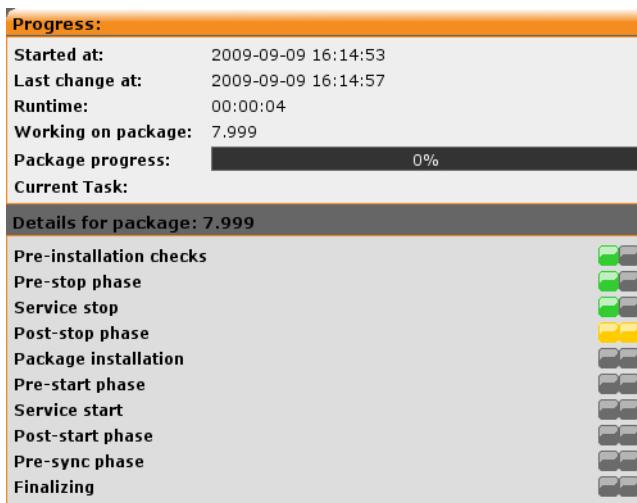


Figure 4.9 Up2Date Progress Bar

define a specific date and time where an update is to be installed automatically. To cancel a scheduled installation, click *Cancel*.

A note on "implicit" installations: There can be a constellation, where you schedule an Up2Date package which requires an older Up2Date package to be installed first. This Up2Date package will be automatically scheduled for installation before the actual Up2Date package. However, you can define a specific time for this package, too, but you cannot prevent its installation.

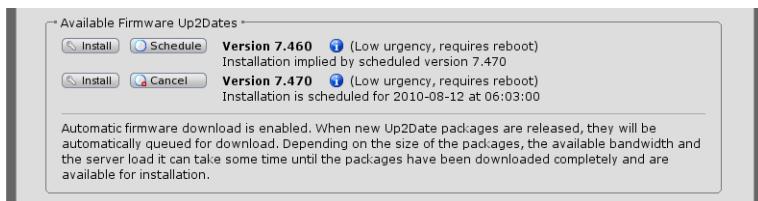


Figure 4.10 Implicit Installation of Up2Date Packages

Pattern

The *Pattern* section shows the current version of the installed patterns. If you have selected *Manual* on the *Configuration* tab, you can see a *Update Patterns Now* button. Use this button to download and install new patterns if available.

Note – The current pattern version does not need to be identical with the latest available pattern version in order for the ASG unit to be working correctly. A

deviation between the current and the latest available pattern version might occur when new patterns are available, which, however, do not apply to the unit you are using. What patterns are downloaded is dependent on your settings and hardware configuration. For example, if you do not use the intrusion prevention feature of Astaro Security Gateway, newly available IPS patterns will not be installed, thus increasing the divergence between the currently installed and the latest available pattern version.

Configuration

By default, new update packages are automatically downloaded to the firewall.

Firmware Download Interval

This option is set to 15 minutes by default, that is Astaro Security Gateway checks every 15 minutes for available firmware updates. Astaro Security Gateway will automatically download (but not install) available firmware update packages. The precise time when this happens is distributed randomly within the limits of the selected interval. You can change the interval up to *Monthly* or you can disable automatic firmware download by selecting *Manual* from the drop-down list. If you select *Manual* you will find a *Check for Up2Date Packages Now* button on the *Overview* tab.

Pattern Download/Installation Interval

This option is set to 15 minutes by default, that is Astaro Security Gateway checks every 15 minutes for available pattern updates. Astaro Security Gateway will automatically download and install available pattern update packages. The precise time when this happens is distributed randomly within the limits of the selected interval. You can change the interval up to *Monthly* or you can disable automatic pattern download and installation by selecting *Manual* from the drop-down list. If you select *Manual* you will find a *Update Patterns Now* button on the *Overview* tab.

Advanced

The *Management >> Up2Date >> Advanced* tab lets you configure further Up2Date options such as selecting a parent proxy or Up2Date cache for your firewall.

Note – Update packages can be downloaded from Astaro's FTP server at <ftp://ftp.astaro.com>.

Manual Up2Date Package Upload: If your firewall does not have direct access to the Internet or an Up2Date cache to download new update packages directly, you can upload the update package manually. To do so, proceed as follows:

1. Open the *Upload File* dialog box.

Click the folder next to the *Up2Date File* box.

The *Upload File* dialog box opens.

2. Select the update package.

Click *Browse* in the *Upload File* dialog box and select the update package you want to upload.

3. Click *Start Upload*.

The update package will be uploaded to the firewall.

4. Click *Apply*.

Your settings will be saved.

Parent Proxy

A parent proxy is often required in those countries that require Internet access to be routed through a government-approved proxy server. If your security policy requires the use of a parent proxy, you can set it up here by selecting the host definition and port.

Use a Parent Proxy: Select the checkbox to enable parent proxy use. Enter the hostname and the port of the proxy.

This Proxy Requires Authentication: If the parent proxy requires authentication, enter username and password here.

If a parent proxy is configured, Astaro Security Gateway fetches both firmware and pattern Up2Dates from it.

Backup/Restore

The backup restoring function allows you to save the settings of the firewall to a file on a local disk. This backup file allows you to install a known good configuration on a new or misconfigured system.

Be sure to make a backup after every system change. This will ensure that the most current settings are always available. In addition, keep your backups in a safe place, as it also contains security-relevant data such as certificates and cryptographic keys. After generating a backup, you should always check it for readability. It is also a good idea to use an external program to generate MD5 checksums, for this will allow you to check the integrity of the backup later on.

Backup/Restore

To create a backup with the current system state, proceed as follows:

1. **Open the *Backup/Restore* tab.**

2. **Enter a comment (optional).**

Add a description or other information about the backup.

3. **Click *Create Backup Now*.**

The backup appears in the available backups list.

There, all backups are listed with information about the date/time of creation, the version number of Astaro Security Gateway Software, and the user who created it.

You can decide whether to *Restore*, *Download*, *Send* or *Delete* a backup. If you select to download a backup, you are prompted to select a location in the file system for the downloaded backup to reside (the file extension for unencrypted backups is **abf**).

If you click *Send* a small dialog window opens where you can decide to send the file encrypted (provide password) or unencrypted. Click *Save* to send the backup. Recipients will be the standard recipients, that is, the backup will be sent to the address(es) provided on the *Automatic Backups* tab.

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

In addition, you have the option to encrypt the backup (Triple DES encryption). Once you have selected this option, provide a password (second time for verification). You will be asked for this password when importing the backup (the file extension for encrypted backups is **ebf**).

Note – A backup does include administrator passwords, the high availability passphrase if configured, as well as all RSA keys and X.509 certificates. Since this information is confidential, it is good practice to enable encryption.

To import a backup, click the folder icon and select a backup file to upload, then click *Start Upload*. When importing an encrypted backup file, you must provide the correct passphrase prior to importing the backup. Note that the backup will not instantly be restored. Instead, it will be added to the *Available Backups* list.

Note that you can also recover unencrypted backup files (file extension abf) from a FAT formatted USB flash drive such as a simple USB stick. To restore a backup from a USB flash drive, copy the backup file to the USB flash drive and plug the device into Astaro Security Gateway prior to boot up. If several backup files are stored on the device, the lexicographically first file will be used (numbers precede letters). For example, suppose the backup files `firewall_backup_2007-04-17.abf` and `2006-03-20_firewall_backup.abf` are both stored on the USB flash drive. During the boot up, the second file will be used because it begins with a number, although it is much older than the other one.

In addition, a lock file is created after the successful recovery of a backup, preventing the installation of the same backup over and over again while the USB flash drive is still being plugged in. However, if you want to install a previous backup once again, you must first reboot with no USB flash drive plugged in. This will delete all lock files. When you now boot with the USB flash drive plugged in again, the same backup can be installed.

Automatic Backups

On the *Management >> Backup/Restore >> Automatic Backup* tab you can configure several options dealing with the automatic generation of backups. To have backups created automatically, proceed as follows:

1. **On the *Automatic Backups* tab, enable the option.**

You can either click the status icon or the *Enable* button.

The status icon turns green and the *Options* and *Send Backups by E-mail* areas become editable.

2. **Select the interval.**

Automatic backups can be created at various intervals.

You can choose between daily, weekly, and monthly.

3. **Specify the maximum number of backups to be stored.**

Backups are stored up to the number you enter here. Once the maximum has been reached, the oldest backups will be deleted.

Note that this applies to automatically created backups only. Backups created manually will not be deleted.

4. Click **Apply**.

Your settings will be saved.

To save you the work of backing up your firewall manually, the backup feature supports e-mailing the backup file to a list of defined e-mail addresses.

Recipients: Automatically generated backups will be sent to users contained in the *Recipients* box. Multiple addresses can be selected. By default, the first administrator's e-mail address is used.

Encrypt E-Mail Backups: In addition, you have the option to encrypt the backup (Triple DES encryption).

Password: Once you have selected the *Encryption* option, provide a password (second time for verification). You will be prompted for this password when importing the backup.

Automatically created backups will appear in the *Available Backups* list on the *Backup/Restore* tab, marked with the *System* flag indicating the creator. From there, they can be restored, downloaded, or deleted as any backup you have created by yourself.

V6 Backup Import

On the *Management >> Backup/Restore >> V6 Backup Import* tab you can upload backups of Astaro Security Gateway version 6.

Note – Only unencrypted backups of ASG Software version 6.303 or higher can be imported. If you have installed an older version, please update to version 6.303 first before creating a backup you intend to import into a unit running version 7.

Also note the following limitations when importing a backup of Astaro Security Gateway V6:

- Only backups of version 6.303 or later are supported.
- HA configuration will not be converted.
- Remote Syslog will not be converted.

- Site-to-site and remote access VPN: Only PPTP settings will be converted.
- Intrusion prevention settings will not be converted.
- Network and service groups: Groups containing other groups will be expanded.
- Packet filter: QoS settings of packet filter rules will not be converted.
- DHCP on Eth-VLAN is unsupported in V7.
- Configured Ethernet aliases that are disabled will not be converted.
- E-mail address fields in V6 (such as *System >> Settings >> Administrator Contact*) will not be converted.
- HTTP proxy configuration will not be converted.
- SMTP proxy configuration will not be converted.
- Remote user authentication services will not be converted.
- DHCP relay will not be converted.

To upload an ASG V6 backup file, proceed as follows:

1. **Open the *V6 Backup Import* tab.**
2. **Select a backup file to upload.**
Click the folder icon and select the backup file you want to upload.
3. **Click *Start Upload*.**
The backup file will be imported.

Note that the backup will not be installed directly. Instead, it will be added to the *Available Backups* list on the *Management >> Backup/Restore* tab. From there, it can be restored, downloaded, or deleted.

Caution – After you have restored an Astaro Security Gateway V6 backup, carefully check your entire settings prior to putting the firewall into operation.

User Portal

The User Portal of Astaro Security Gateway is a special browser-based application on the unit providing personalized e-mail and remote access services to authorized users. It can be accessed by browsing to the URL of Astaro Security Gateway, for example, <https://192.168.2.100> (note the HTTPS protocol and the missing port number 4444 you would normally enter for accessing the WebAdmin interface).

Among other things, the User Portal contains the e-mail quarantine, which holds messages that are infected by malicious software, contain suspicious attachments, are identified as spam, or contain certain expressions you have explicitly declared forbidden.

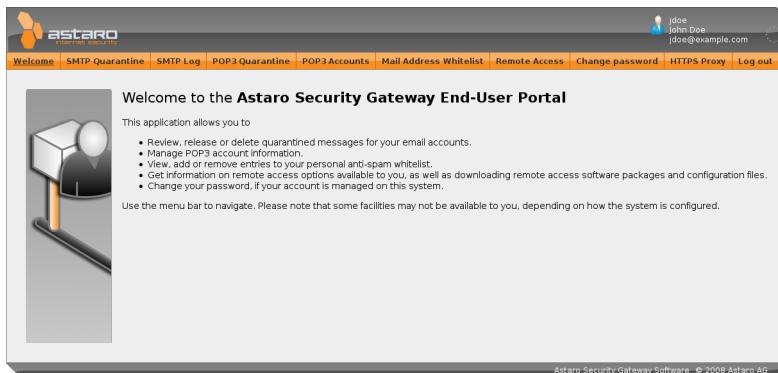


Figure 4.11 User Portal of Astaro Security Gateway

On the User Portal, users have access to the following services:

- **SMTP Quarantine:** Users can view and release messages held in quarantine. Which types of messages they are allowed to release can be determined on the *Mail Security >> Quarantine Report >> Advanced* tab.
- **SMTP Log:** Here, users can view the SMTP log of their mail traffic.
- **POP3 Quarantine:** Users can view and release messages held in quarantine. Which types of messages they are allowed to release can be determined on the *Mail Security >> Quarantine Report >> Advanced* tab.
- **POP3 Accounts:** Users can enter their credentials of POP3 accounts they use. Only those spam e-mails will appear in the User Portal for which POP3 account credentials are given. A user for whom POP3 account credentials

are stored will receive an individual Quarantine Report for each e-mail address. Note that allowed POP3 servers must be specified on the *Mail Security >> POP3 >> Advanced* tab.

- **Mail Address Whitelist:** Here, senders can be whitelisted, thus messages from them are not regarded as spam. Whitelisted senders can be specified by either entering valid e-mail addresses (e.g., jdoe@example.com) or all e-mail addresses of a specific domain using an asterisk as wildcard (e.g., *@example.com).
- **Remote Access:** Users can download remote access client software and configuration files provided for them. However, the *Remote Access* tab is only available if at least one remote access mode has been enabled for the specific user.

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

- **Change Password:** Users can change the password for accessing the User Portal.
- **Log Out:** Click here to log out of the User Portal. This is only necessary when you have selected *Remember My Login* at login (which creates a cookie) and you want to explicitly logout and have this cookie deleted. Otherwise, there is no need to use the logout button—closing the browser tab or window is sufficient.

Global

On the *Management >> User Portal >> Global* tab you can specify from which networks access to the user is to be granted.

To enable User Portal access, proceed as follows:

1. **Enable the User Portal.**

You can either click the status icon or the *Enable* button.

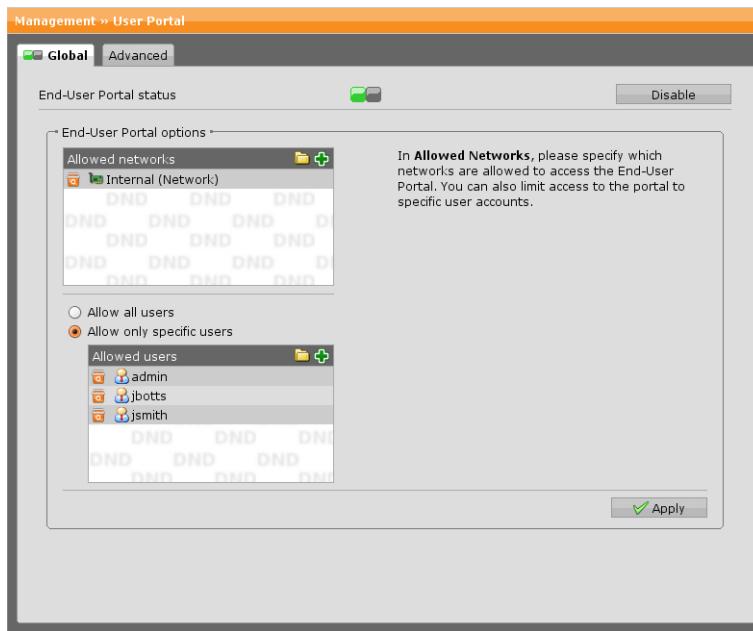


Figure 4.12 Configuring Access to the User Portal

The status icon turns amber and the *User Portal Options* area becomes editable.

2. Select the allowed networks.

Select the networks that should be allowed to access the User Portal.

3. Select the allowed users.

Select the users or user groups that should be able to access the User Portal. If you do not want to grant access to all users, click *Allow Only Specific Users* and select the users and user groups individually.

4. Click **Apply**.

Your settings will be saved.

Advanced

On the *Advanced* tab you can configure an alternative hostname and port number for the User Portal as well as language and security options.

Language

During login, the User Portal fetches the language settings of the web browser

and loads the respective locales to display the portal in the same language as the browser defaults. For browser language settings that are not available for the User Portal, you can select here which language will be the fallback language.

Security

The User Portal uses cookies to track sessions. Persistent cookies permit to return after having closed a session without having to log in again. They can always be deleted from user-side, however, by using the *Log Out* button of the User Portal.

Disable Portal Items

For the features listed here a menu item is displayed in the User Portal when the respective feature has been enabled in WebAdmin. However, here you can define menu items that should *not* be displayed in the User Portal. To do so, select the respective option(s) and click *Apply*.

Hostname and Port

By default, this is the firewall's hostname as given on the *Management >> System Settings >> Hostname* tab. However, it is possible to specify an alternative portal hostname.

By default, port 443 for HTTPS is selected. You can change the port to either 80 or any value in the range from 1024 to 65535. Note that you cannot select either 10443 or the *WebAdmin TCP Port*, which is configured on the *Management >> WebAdmin Settings >> General* tab.

The daily Quarantine Report, for example, which is sent by the firewall, contains hyperlinks a user can click to release messages from the e-mail quarantine. By default, these links point to the hostname of the firewall. However, if you want to grant access to the User Portal for users gaining access over the Internet, it might be useful to enter an alternative hostname here that can be resolved publicly.

Welcome Message

You can customize the welcome message of the User Portal. Simple HTML markup and hyperlinks are allowed.

Note – Changing the welcome message is not possible when using a home use license.

Notifications

Astaro Security Gateway comes with a notification feature that informs you immediately about all sorts of security-relevant events occurring on the firewall, either by e-mail or SNMP trap. All events that might possibly be of interest to an administrator are represented by various error, warning, and information codes. What notifications are sent depends on the selection you have configured on the *Notifications* tab.

Global

On the *Management >> Notifications >> Global* tab you can configure the sender address (i.e., the *From* address) to be taken for notification e-mails sent by the firewall. By default, this is `do-not-reply@fw-notify.net`. If you want to change this address, it is advisable to enter an e-mail address of your domain, as some mail servers might be configured to check whether a given sender address really exists.

In addition, you can specify the recipients of firewall notifications. By default, this is the administrator's e-mail address you had entered during the initial setup.

Limit Notifications: Some security-relevant events such as detected intrusion attempts will create a lot of notifications, which may quickly clog the notification recipients' e-mail inboxes. For this reason, Astaro Security Gateway has sensible default values to limit the number of notifications sent per hour. If you disable this option, every security-relevant event will create a notification, provided the event is configured so as to send a notification on the *Management >> Notifications >> Notifications* tab.

Device Specific Text

Here you can enter a description of the Astaro Security Gateway, e.g. its location, which will be displayed in the notifications sent.

Notifications

Notifications are divided into three categories:

- **CRIT:** Messages informing about critical events that might render the firewall inoperable.
- **WARN:** Warnings about potential problems that need your attention, for example, exceeding thresholds.
- **INFO:** Merely informational messages such as the restart of a system component, for example.

You can select whether you want to send the notification as e-mail or SNMP trap.

Advanced

In case your ASG cannot send e-mails directly, you can configure a smarthost to send the e-mails. Proceed as follows:

1. **Enable External SMTP on the Management >> Notifications >> Advanced tab.**

You can either click the status icon or the *Enable* button.

2. **Enter your smarthost.**

You can use drag-and-drop. The port is preset to the default SMTP port 25.

- **Use TLS:** Select this checkbox if you want to enforce TLS when sending notifications.

Note that notifications will not be sent if the smarthost does not support TLS.

3. **Click *Apply*.**

Your settings will be saved.

If the smarthost requires authentication, enter the corresponding username and password for the smarthost in the *Authentication* area below. Click *Apply* to save your settings.

Customization

The tabs of the *Management >> Customization* menu allow you to customize and localize the templates of status messages and e-mail notifications created by Astaro Security Gateway, allowing you to adapt those messages to the policy and corporate identity of your company.

Note – Customization is not possible when using a home use license.

Global

On the *Management >> Customization >> Global* tab you can customize global displaying options for the system messages presented to users. Note that UTF-8/Unicode is supported.

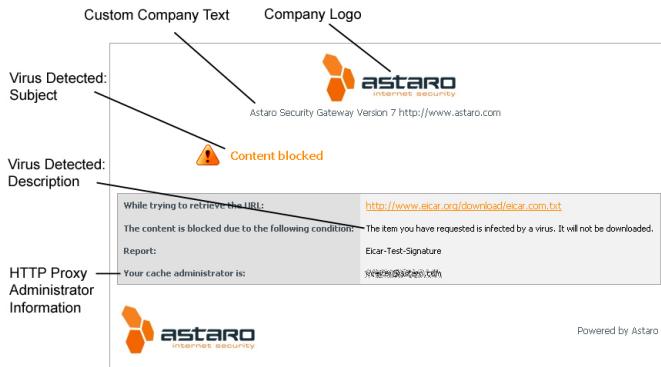


Figure 4.13 Example Warning Page and its Customizable Parts

Company Logo: You can upload your own logo/banner (in jpg format only), which is used in the following contexts:

- HTTP/S status messages
- POP3 blocked pages
- Quarantine release status messages (which will appear after a spam e-mail has been released or whitelisted from the quarantine through the Quarantine Report)
- Quarantine Report

Restrict the image's resolution to a reasonable value (e.g., 100 x 200 pixels).

To upload a banner, proceed as follows:

1. Open the *Upload File* dialog box.

Click the folder icon next to the *Upload New Logo* box.

The *Upload File* dialog box opens.

2. Select the banner.

Browse to the location where the banner you want to upload resides.

Once you have selected the banner, click *Start Upload*.

3. Click *Apply*.

The banner will be uploaded replacing the file already installed.

Custom Company Text: Customize the message that will be displayed beneath the company logo whenever a website was blocked by the virus scanner or the

content filter of Astaro Security Gateway. For example, you might want to enter the administrator's contact data here. Note that blocking of a website might have various reasons, for example, if it belongs to a category that is forbidden or classified as spyware, or if a user tries to download a file whose extension is considered critical (e.g., executables). Templates used for these occurrences can be modified on the *Management >> Customization >> HTTP/S Proxy* tab.

HTTP/S Proxy

Customize the templates for warning web pages of the HTTP/S proxy of Astaro Security Gateway that will be displayed when attempts to access banned websites are detected, providing different warning notes for each type of transgression. You can translate these templates into other languages or modify them to show customer support contact information, for example. The following message templates can be customized:

- **HTTP Proxy Administrator Information:** Here you can enter information about the administrator managing the HTTP/S proxy. In addition, you can enter the administrator's e-mail address.
- **Content Blocked by Surf Protection:** This message is displayed when a user had attempted to access a web page whose contents matched a URL category that is configured to be blocked.
- **Content Blocked by Blacklist:** This message is displayed when a user had attempted to retrieve a web page whose contents matched a URL that is blacklisted. To blacklist URLs, see *Web Security >> HTTP/S >> URL Filtering*.
- **Virus Detected:** This message is shown when a file was blocked due to a virus infection.
- **Downloading File:** This message is shown when a file download is in progress.
- **Virus Scanning:** This message is shown while a file is being scanned for malicious content.
- **File Download Completed:** This message is shown after a file has been fully downloaded and scanned.
- **Transparent Mode with Authentication:** This section is only meaningful if you use the proxy in *Transparent Mode with Authentication*. The text

is displayed on the authentication page where every user needs to log in before they can use the proxy. The *Terms of Use* field is empty by default, which means that no disclaimer is presented on the authentication page. However, if you want to add a disclaimer which users have to accept, fill in this field. You can disable the disclaimer again by emptying the *Terms of Use* field.

Download Manager

If the HTTP/S proxy is enabled, the web browser will display the following downloader pages while downloading content > 1 MB in size and whose content type is no text or image. Note that the downloader page will not be displayed when video or audio streams are being requested or more than 50% of the file has been downloaded within five seconds.

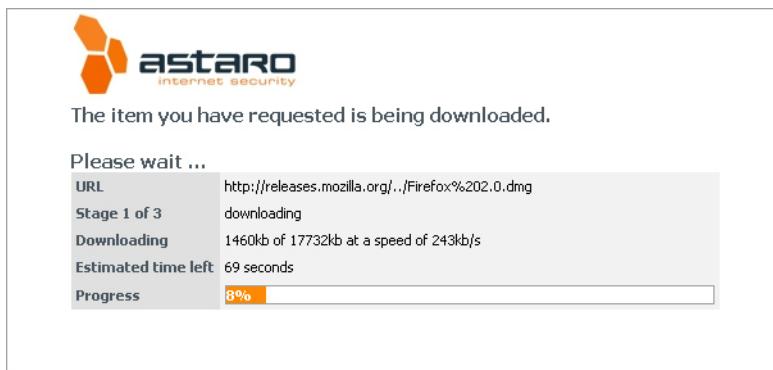


Figure 4.14 HTTP Downloader Page Step 1 of 3

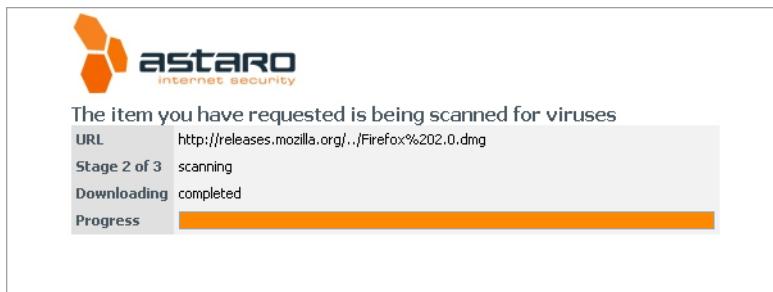


Figure 4.15 HTTP Downloader Page Step 2 of 3

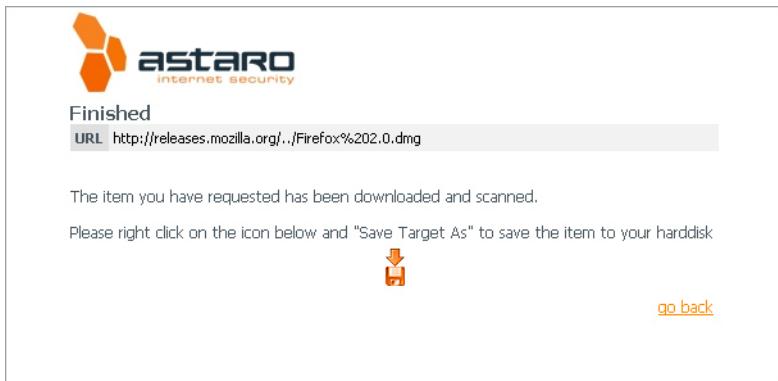


Figure 4.16 HTTP Downloader Page Step 3 of 3

SMTP/POP3 Proxy

Customize the templates to be used in user messages generated by the SMTP/POP3 proxies of Astaro Security Gateway. You can translate these templates into other languages or modify them as to show customer support contact information, for example. The following message templates can be customized:

- **Message Released From Quarantine:** This message is shown when an e-mail was successfully released from the quarantine.
- **Error While Releasing Message From Quarantine:** This message is shown when an error occurred while releasing a message from the quarantine.
- **POP3 Message Blocked:** This message is shown when a POP3 e-mail was blocked.

SNMP

The *Simple Network Management Protocol* (SNMP) is used by network management systems to monitor network-attached devices such as routers, servers, and switches. SNMP allows the administrator to make quick queries about the condition of each monitored network device. You can configure Astaro Security Gateway to reply to SNMP queries or to send SNMP traps to SNMP management tools. The former is achieved with so-called management information bases (MIBs). An MIB specifies what information can be queried for which network device. Astaro Security Gateway supports the following MIBs:



Figure 4.17 POP3 Blocked Message

- **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)

In order to get Astaro Security Gateway system information, an SNMP manager must be used that has at least the RFC1213-MIB (MIB II) compiled into it.

Query

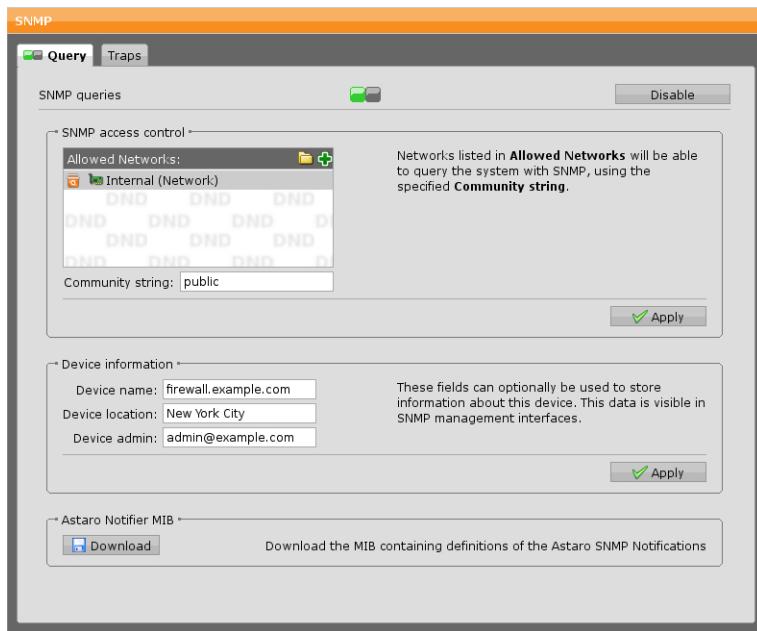


Figure 4.18 Configuring SNMP Queries

To configure SNMP queries, proceed as follows:

1. **Enable *SNMP Queries*.**

You can either click the status icon or the *Enable* button.

2. **Select *Allowed Networks*.**

Networks listed in the *Allowed Networks* box are able to query the SNMP agent running on Astaro Security Gateway. Note that the access is always read-only.

3. **Enter a community string.**

An SNMP community string acts as a password that is used to protect access to the SNMP agent.

By default, the SNMP community string is "public", but you can change it to any setting that best suits your needs.

Note – Allowed characters for the community string are: (a–z), (A–Z), (0–9), (+), (_), (@), (.), (-), (blank).

4. Click **Apply**.

Your settings will be saved.

Furthermore, you can enter additional information about the firewall.

Device Information

The *Device Information* text boxes can be used to specify additional information about the firewall such as its name, location, and administrator. This information can be read by SNMP management tools to help identify the firewall.

Note – All SNMP traffic (protocol version 2) between the firewall and the *Allowed Networks* is not encrypted and can be read during the transfer over public networks.

Astaro Notifier MIB

This section allows you to download the Astaro notifier management information base (MIB) which contains the definitions of the Astaro SNMP notification based on your current settings for the notification traps.

Traps

In the *Traps* tab you can define an SNMP trap server to which notifications of relevant events occurring on the firewall can be sent as SNMP traps. Note that special SNMP monitoring software is needed to display those traps.

The messages that are sent as SNMP traps contain so-called object identifiers (OID), for example, .1.3.6.1.4.1.9789, which belong to the private enterprise numbers issued by IANA¹³. Note that .1.3.6.1.4.1 is the iso.org.dod.internet.private.enterprise prefix, while 9789 is Astaro's *Private Enterprise Number*. The OID for notification events is 1500, to which are appended the OIDs of the type of the notification and the corresponding error code (000-999). The following notification types are available:

- DEBUG = 0
- INFO = 1

¹³ <http://www.iana.org>

- **WARN** = 2
- **CRIT** = 3

Example: The notification "INFO-302: New firmware Up2Date installed" will use the OID .1.3.6.1.4.1.9789.1500.1.302 and has the following string assigned:

[<HOST>][INFO][302]

Note that <HOST> is a placeholder representing the hostname of the system and that only type and error code from the notification's subject field are transmitted.

To select a SNMP trap server, proceed as follows:

1. **Click *New SNMP Trap Sink*.**

The *Create New SNMP Trap Sink* dialog box opens.

2. **Make specific settings for this SNMP trap sink.**

Host: The host definition of the SNMP trap server.

Community string: An SNMP community string acts as a password that is used to protect access to querying SNMP messages. By default, the SNMP community string is set to "public". Change it to the string that is configured on the remote SNMP trap server.

Note – Allowed characters for the community string are: (a–z), (A–Z), (0–9), (+), (_), (@), (.), (-), (blank).

Comment (optional): Add a description or other information about the SNMP trap server.

3. **Click *Save*.**

The new SNMP trap server will be listed on the *Traps* tab.

Central Management

The pages of the Central Management menu let you configure interfaces to management tools that can be used to monitor or remotely administer the firewall.

Astero Command Center

Astero Command Center (ACC) is Astero's central management product. It provides features such as monitoring, configuration, maintenance, inventory, and the possibility of multiple administrators. It is intended to provide a general overview of the state of each Astero gateway software and appliance installation, their version, current load, license expiration, and critical security events. The information is accessible via a graphical web-based frontend providing you with various view options for all monitored devices. In addition, ACC includes an inventory system that automatically keeps track of each device. Finally, you can assign different administrative privileges for multiple administrators, thus making ACC the perfect solution for Astero partners and MSSPs. For more information on Astero Command Center, please refer to the ACC data sheet, which is available at the Astero website¹⁴.

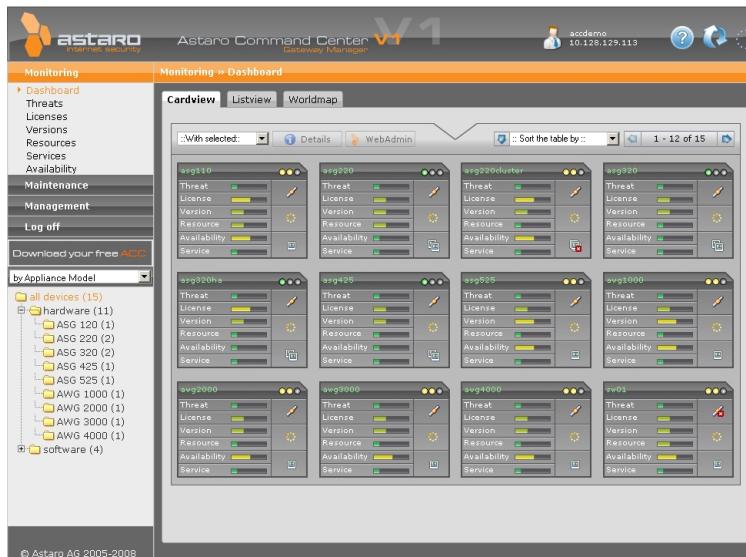


Figure 4.19 Dashboard of Astero Command Center

¹⁴ http://www.astero.com/our_products/management_tools/astero_command_center

Setting up ACC V2.0

To prepare Astaro Security Gateway to be monitored by an ACC server, proceed as follows:

1. On the Astaro *Command Center* tab, enable ACC.

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *ACC Settings* area becomes editable.

2. Set the managing ACC server version to ACC V2.x (default).

All input fields on this page become fully accessible.

3. Specify the ACC Host.

Select or add the ACC server to which Astaro Security Gateway should connect to.

4. Click *Apply*.

Your settings will be saved and the authentication fields become editable.

- Define whether your ACC server requires authentication (optional).**

Select the checkbox *Authentication* and enter the same password (*Shared Secret*) as configured on the ACC server.

- Select ACC server as Up2Date cache (optional).**

Up2Date packages can be fetched from a cache located on the ACC server. If you want to use this functionality for your firewall, select the option *Use ACC Server as Up2Date Cache*. Please ensure that the administrator of your managing ACC has enabled the Up2Date Cache functionality on the server accordingly. Note that usage of the Up2Date Cache functionality is mutually exclusive with using a parent proxy configuration for Up2Dates.

5. Click *Apply*.

Your settings will be saved. Shortly thereafter, Astaro Security Gateway can be monitored and administered by the ACC server selected here. You will be able to see the current connection status and health in the section called *ACC Health*. Reloading the page will update this data. Please use the *Open Live Log* button to further help you diagnose connection problems should they occur.

Note – The communication between the firewall and ACC takes place on port 4433, whereas the Astaro Command Center V1.9 can be accessed through a

browser via the HTTPS protocol on port 4444 for the WebAdmin and on port 4422 for the Gateway Manager interface.

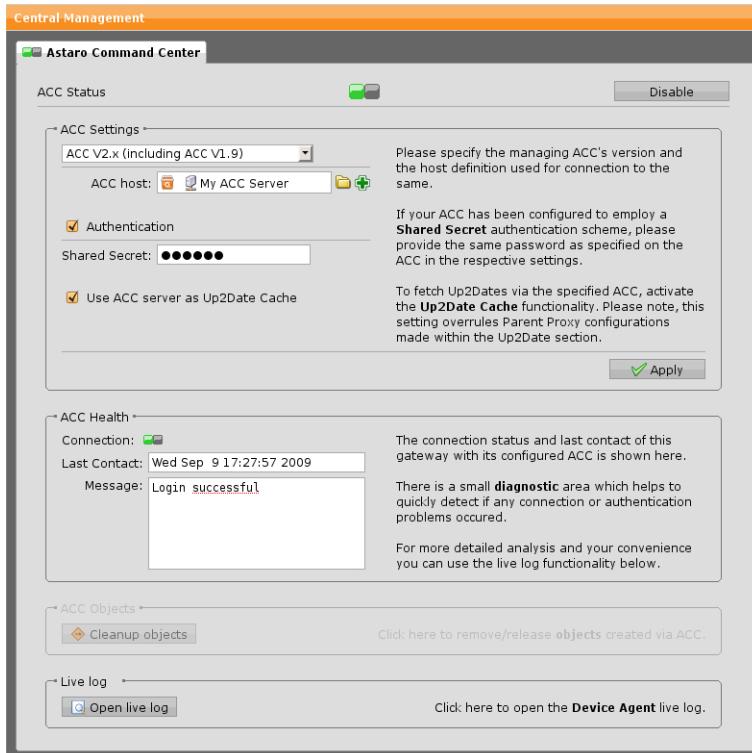


Figure 4.20 Configuring Central Management Using an ACC V1.9 Server

Setting up ACC V1.4

To prepare Astaro Security Gateway to be monitored by an ACC V1.4 Server, proceed as follows:

1. **On the Astaro Command Center tab, enable ACC.**

You can either click the status icon or the *Enable* button.

The status icon turns amber and the ACC *Settings* area becomes editable.

2. **Set the managing ACC Server version to ACC V1.4.**

Non-applicable input fields will be deactivated.

3. Specify the ACC Host.

Select or add the ACC server to which Astaro Security Gateway should connect to.

4. Click Apply.

Your settings will be saved and the authentication fields become editable.

- **Define whether your ACC server requires authentication (optional).**

Select the checkbox *Authentication* and enter the same password (*Shared Secret*) as configured on the ACC server.

- **Select ACC server as Up2Date cache (optional).**

Up2Date packages can be fetched from a cache located on the ACC server. If you want to use this functionality for your firewall, select the option *Use ACC Server as Up2Date Cache*. Please ensure that the administrator of your managing ACC has enabled the Up2Date Cache functionality on the server accordingly. Note that usage of the Up2Date Cache functionality is mutually exclusive with using a parent proxy configuration for Up2Dates.

5. Click Apply.

Your settings will be saved. Shortly thereafter, Astaro Security Gateway can be monitored and administered by the ACC server selected here. Please use the *Open Live Log* button to help you detect connection problems should they occur.

Note – The communication between Astaro Security Gateway and the ACC takes place on port 4433, whereas the Astaro Command Center V1.4 can be accessed through a browser via the HTTPS protocol on port 443.

ACC Objects

The *ACC Objects* area is disabled (grayed-out) unless there are objects that have been created via an ACC and if this ACC is now disconnected from the Astaro Security Gateway. ACC-created objects can be network definitions, remote host definitions, IPSec VPN tunnels, etc.

The button *Cleanup Objects* can be pressed to release any objects that were created by the ACC the device has formerly been managed with. These objects are normally locked and can only be viewed on the local device. After pressing

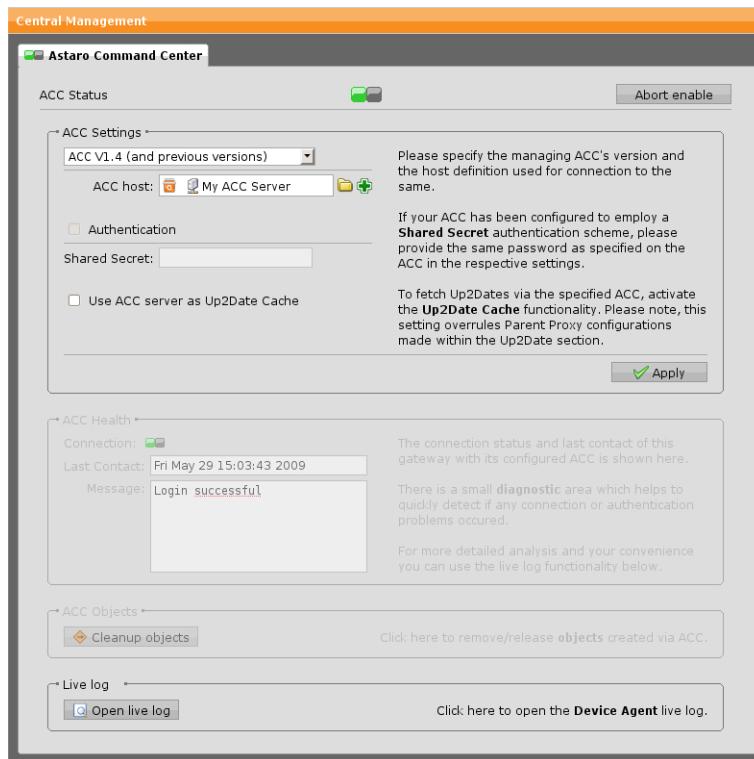


Figure 4.21 Configuring Central Management Using an ACC V1.4 Server

the button, the objects become fully accessible and can be reused or deleted by a local administrator.

Note – In case former ACC-created objects are cleaned up, they cannot be re-transformed when reconnecting to that same ACC. This means that if the remote ACC still hosts object definitions for a device which later re-establishes a connection to it, those objects will be deployed to the device again—although local copies will then already exist.

Live Log

You can use the live log to monitor the connection between your Astaro Security Gateway and the ACC. Click the *Open Live Log* button to open the live log in a new window.

High Availability

The main cause for an Internet security system to fail is because of a hardware failure. The ability of any system to continue providing services after a failure is called failover. Astaro Security Gateway provides high availability (HA) failover, allowing you to set up a hot standby system in case the primary system fails (active-passive). Alternatively, you can use Astaro Security Gateway to set up a cluster, which operates by distributing dedicated network traffic to a collection of nodes (active-active) similar to conventional load-balancing approaches in order to get optimal resource utilization and decrease computing time.

The concepts *high availability* and *cluster* as implemented in Astaro Security Gateway are closely related. For a high availability system can be considered a two-node cluster, which is the minimum requirement to provide redundancy.

Each node within the cluster can assume one of the following roles:

- **Master:** The primary system in a hot standby/cluster setup. Within a cluster, the master is responsible for synchronizing and distributing of data.
- **Slave:** The standby system in a hot standby/cluster setup which takes over operations if the master fails.
- **Worker:** A simple cluster node, responsible for data processing only.

All nodes monitor themselves by means of a so-called heartbeat signal, a periodically sent multicast UDP packet used to check if the other nodes are still alive. If any node fails to send this packet due to a technical error, the node will be declared *dead*. Depending on the role the failed node had assumed, the configuration of the setup changes as follows:

- If the master node fails, the slave will take its place and the worker node with the highest ID will become slave.
- If the slave node fails, the worker node with the highest ID will become slave.
- If a worker node fails, you may notice a performance decrease due to the lost processing power. However, the failover capability is not impaired.

Reporting

All reporting data is consolidated on the master node and is synchronized to the other cluster nodes at intervals of five minutes. In case of a takeover, you will therefore lose not more than five minutes of reporting data. However, there is a distinction in the data collection process. The graphs displayed in the *Reporting >> Hardware* tabs only represent the data of the node currently being master. On the other hand, accounting information such as shown on the *Network Usage* page represents data that was collected by all nodes involved. For example, today's CPU usage histogram shows the current processor utilization of the master node. In the case of a takeover, this would then be the data of the slave node. However, information about top accounting services, for example, is a collection of data from all nodes that were involved in the distributed processing of traffic that has passed the unit.

Notes

- Interface types with dynamic IP address assignment such as PPPoE and Cable Modem (DHCP) are not supported in cluster mode (active/active).
- The *Address Resolution Protocol* (ARP) is only used by the actual master. That is to say, slave and worker nodes do not send or reply to ARP requests.
- In case of a failover event, the unit that takes over operations performs an ARP announcement (also known as *gratuitous ARP*), which is usually an ARP request intended to update the ARP caches of other hosts which receive the request. Gratuitous ARP is utilized to announce that the IP of the master was moved to the slave.
- All interfaces configured on the master must have a physical link, that is, the port must be properly connected to any network device.

Hardware and Software Requirements

The following hardware and software requirements must be met to provide HA failover or cluster functionality:

- Valid license with the high availability option enabled (for the stand-by unit you only need an additional base license).
- Two ASG units with identical software versions and hardware or two ASG appliances of the same model.
- Heartbeat-capable Ethernet network cards. Check the *Hardware Compatibility List* (HCL) to figure out which network cards are supported. The HCL is available at Astaro's knowledgebase¹⁵ (use "HCL" as search term).
- Ethernet crossover cable (for connecting master and slave in a hot standby system). ASG appliance models 320, 425, and 525, whose dedicated HA interface is a Gigabit auto-MDX device, can be connected through a standard IEEE 802.3 Ethernet cable as the Ethernet port will automatically exchange send/receive pairs.
- Network switch (for connecting cluster nodes).

Status

The screenshot shows a web-based management interface for high availability. At the top, there is a navigation bar with tabs: 'Status' (which is selected), 'System Status', and 'Configuration'. Below the navigation bar, a message states: 'System is currently in operation mode: Cluster'. To the right of this message is a link labeled 'Open HA live log'. The main content area is a table with the following data:

ID	Role	Device Name	Status	Version	Last Status Change	Reboot	Shutdown
1	SLAVE	Node1	ACTIVE	7.490	Wed Sep 9 14:51:54 2009	<input type="button" value="Reboot"/>	<input type="button" value="Shutdown"/>
2	MASTER	Node2	ACTIVE	7.490	Wed Sep 9 14:25:57 2009	<input type="button" value="Reboot"/>	<input type="button" value="Shutdown"/>
3	WORKER	Node3	ACTIVE	7.490	Wed Sep 9 14:26:10 2009	<input type="button" value="Reboot"/>	<input type="button" value="Shutdown"/>
4	WORKER	Node4	ACTIVE	7.490	Wed Sep 9 14:37:22 2009	<input type="button" value="Reboot"/>	<input type="button" value="Shutdown"/>

Figure 4.22 High-Availability Status

The *Management >> High Availability >> Status* tab lists all devices involved in a hot standby system or cluster and provides the following information:

- **ID:** The device's node ID. In a hot standby system, the node ID is either 1 (master) or 2 (slave).
The node ID in a cluster can range from 1–10, as a cluster can have up to a maximum of 10 nodes.
- **Role:** Each node within the cluster can assume one of the following roles:

¹⁵ <http://www.astaro.com/kb/>

- **MASTER:** The primary system in a hot standby/cluster setup. It is responsible for synchronizing and distributing of data within a cluster.
- **SLAVE:** The standby system in a hot standby/cluster setup which takes over operations if the master fails.
- **WORKER:** A simple cluster node, responsible for data processing only.
- **Device Name:** The name of the device.
- **Status:** The state of the device concerning its HA status; can be one of the following:
 - **ACTIVE:** The node is fully operational.
 - **UNLINKED:** One or more interface links are down.
 - **UP2DATE:** An Up2Date is in progress.
 - **UP2DATE-FAILED:** An Up2Date has failed.
 - **DEAD:** The node is not reachable.
 - **SYNCING:** Data Synchronization is in progress. This status is displayed when a takeover process is going on. The initial synchronizing time is at least 5 minutes. It can, however, be lengthened by all synchronizing-related programs. While a SLAVE is synchronizing and in state *SYNCING*, there is no graceful takeover, e.g. due to link failure on master node.
- **Version:** Version number of Astaro Security Gateway Software installed on the system.
- **Last Status Change:** The time when the last status change occurred.

Reboot/Shutdown: With these buttons, a device can be manually rebooted or shut down.

Remove Node: Use this button to remove a dead cluster node via WebAdmin. All node-specific data like mail quarantine and spool is then taken over by the master.

Click the button *Open HA Live Log* in the upper right corner to open the high availability live log in a separate window.

System Status

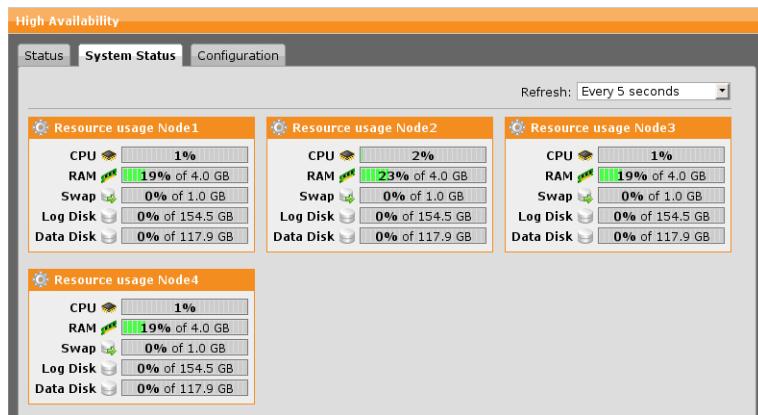


Figure 4.23 Resource Usage of the Single HA or Cluster Devices

The *Management >> High Availability >> System Status* tab lists all devices involved in a hot standby system or cluster and provides information about the resource usage of each device:

- The CPU utilization in percent
- The RAM utilization in percent
- The Swap utilization in percent
- The amount of disk space consumed by the log partition in percent
- The amount of disk space consumed by the root partition in percent

Configuration

The high availability functionality of Astaro Security Gateway covers three basic settings:

- Automatic Configuration
- Hot standby (active-passive)
- Cluster (active-active)

Automatic Configuration: Astaro Security Gateway features a plug-and-play configuration option for ASG appliances that allows the setup of a hot standby

system/cluster without requiring reconfiguration or manual installation of devices to be added to the cluster. Simply connect the dedicated HA interfaces (eth3) of your ASG appliances with one another, select *Automatic Configuration* for all devices, and you are done.

Note – For *Automatic Configuration* to work, all ASG appliances must be of the same model. For example, you can only use two ASG 320 appliances to set up a HA system; one ASG 220 unit on the one hand and one ASG 320 unit on the other hand cannot be combined.

If you connect two ASG appliances through this dedicated interface, all devices will recognize each other and configure themselves automatically as an HA system—the device with the longer uptime becoming master. If the unlikely case should occur that the uptime is identical, the decision which device is becoming master will be made based on the MAC address.

Using ASG Software, the *Automatic Configuration* option is to be used on dedicated slave systems to automatically join a master or already configured hot standby system/cluster. For that reason, *Automatic Configuration* can be considered a transition mode rather than a high availability operation mode in its own right. For the high availability operation mode will change to *Hot Standby* or *Cluster* as soon as a device with *Automatic Configuration* selected joins a hot standby system or cluster, respectively. The prerequisite, however, for this feature to work is that the option *Autojoin* is enabled on the master system. The *Autojoin* function will make sure that those devices will automatically be added to the hot standby system/cluster whose high availability operation mode is set to *Automatic Configuration*.

Hot Standby (active-passive): Astaro Security Gateway features a hot standby high availability concept consisting of two nodes, which is the minimum required to provide redundancy. One of the major improvements introduced in Astaro Security Gateway Software V7 is that the latency for a takeover could be reduced to less than two seconds. In addition to packet filter connection synchronization, the firewall also provides IPSec tunnel synchronization. This means that roadwarriors as well as remote VPN gateways do not need to re-establish IPSec tunnels after the takeover. Also, objects residing in the quarantine are also synchronized and are still available after a takeover.

Cluster (active-active): To cope with the rising demand of processing large volumes of Internet traffic in real time, Astaro Security Gateway features a clustering functionality that can be employed to distribute processing-intensive

tasks such as content filtering, virus scanning, intrusion detection, or decryption equally among multiple cluster nodes. Without the need of a dedicated hardware-based load balancer, the overall performance of the firewall can be increased considerably.

Note – When configuring a cluster, make sure you have configured the master node first before connecting the remaining units to the switch.

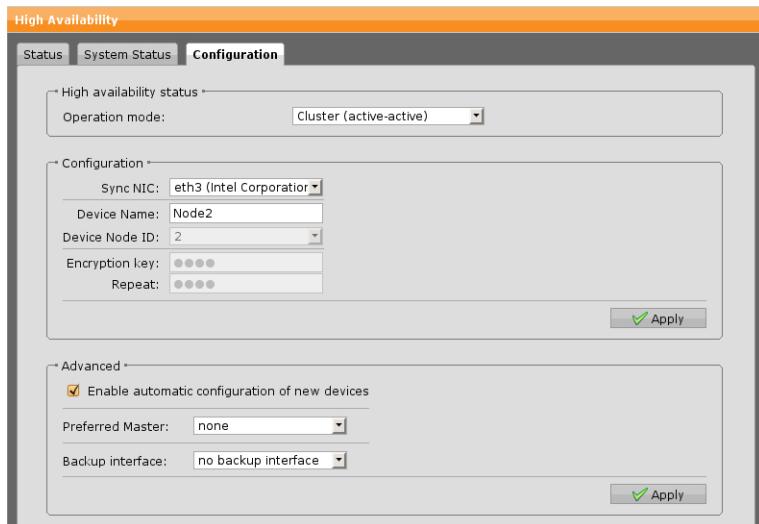


Figure 4.24 Configuring a Cluster

To set up the master of hot standby system/cluster, proceed as follows:

1. **Select a high availability operation mode.**

By default, high availability is turned off.

The following modes are available:

- o Automatic Configuration
- o Hot Standby (active-passive)
- o Cluster (active-active)

Either select *Hot Standby* or *Cluster*.

Note – If you want to change the high availability operation mode, you must always set the mode back to *Off* before you can change it to either *Automatic Configuration*, *Hot Standby*, or *Cluster*.

2. Make the following settings:

Sync NIC: Select the network interface card through which master and slave systems will communicate. If link aggregation is active you can select here a link aggregation interface, too.

Note – Only those interfaces are displayed that have not been configured yet.

The following options can only be configured if you either select *Hot Standby* or *Cluster* as operation mode.

Device Name: Enter a descriptive name for this device.

Device Node ID: Select the node ID of the device. In a case of a failure of the primary system, the node with the highest ID will become master.

Encryption Key: The passphrase with which the communication between master and slave is encrypted (enter the passphrase twice for verification). Maximum key length is 16 characters.

3. Click **Apply**.

The high-availability failover is now active on the master.

4. Optionally, make the following advanced settings:

Autojoin: If you have configured a hot standby system/cluster manually, the *Autojoin* function will make sure that those devices will automatically be added to the hot standby system/cluster whose high-availability operation mode is set to *Automatic Configuration*.

Note – In case of a failure of the HA synchronization interface, no configuration is synchronized anymore. The backup interface only prevents master-master situations.

5. Click **Apply**.

Your settings will be saved.

Now, continue setting up the slave system:

1. Select a high availability operation mode.

By default, high availability is turned off.

The following modes are available:

- Automatic Configuration
- Hot Standby
- Cluster

If you select Automatic Configuration, you only need to select the interface to communicate with the master.

2. Make the following settings:

Sync NIC: Select the network interface card through which master and slave systems will communicate. If link aggregation is active you can select here a link aggregation interface, too. The following options can only be configured if you either select *Hot Standby* or *Cluster* as operation mode.

Device Name: Enter a descriptive name for this device.

Device Node ID: Select the node ID of the device. In a case of a failure of the primary system, the node with the highest ID will become master.

Encryption Key: The passphrase with which the communication between master and slave is encrypted (enter the same passphrase as configured on the master). Maximum key length is 16 characters.

3. Click *Apply*.

The high-availability failover is now active on the master.

4. Optionally, make the following advanced settings:

Autojoin: If you have configured a hot standby system/cluster manually, the *Autojoin* function will make sure that those devices will automatically be added to the hot standby system/cluster whose high-availability operation mode is set to *Automatic Configuration*. However, this option is of no effect on slave systems, so you can leave it enabled, which is the default setting.

Note – In case of a failure of the HA synchronization interface, no configuration is synchronized anymore. The backup interface only prevents master-master situations.

5. Click **Apply**.

Your settings will be saved.

The firewall in hot standby mode will be updated at regular intervals over the data transfer connection. Should the active primary system encounter an error, the secondary will immediately and automatically change to normal mode and take over the primary system's functions.

Note – When you deactivate a hot standby system/cluster, the slave and worker nodes will perform a factory reset and shut down.

More information (especially use cases) can be found in the *HA/Cluster Guide*, which is available at Astaro's knowledgebase¹⁶.

Configuration

It is possible to change the synchronization interface in a running configuration. Note that afterwards all nodes are going to reboot.

Advanced

This section allows you to make some advanced settings.

Enable Automatic Configuration of New Devices: This option is active by default and takes care that newly attached devices are going to be configured automatically.

Preferred Master: Here you can define a designated master node by selecting a node from the drop-down list. In case of a failover, the selected node will not stay in Slave mode after the link recovers but instead will switch back to Master mode.

Backup Interface: To prevent that both master and slave become master at the same time (master-master situations), for example, because of a failure of the HA synchronization interface or an unplugged network cable, a backup heartbeat interface can be selected. This additional heartbeat interface can be any of the configured and active Ethernet interfaces. If a backup interface is selected, an additional heartbeat signal is sent via this interface in one direction from the master to the slave to make sure that the master-slave configuration stays intact. If the master-slave connection is disabled and the backup interface becomes involved, the administrator will receive a notification informing that one of the cluster nodes is dead. However, this option is of no effect on slave systems, so you can leave it unconfigured.

¹⁶ <http://www.astaro.com/kb/>

Shutdown and Restart

On this tab you can manually shut down or restart Astaro Security Gateway.

Shutdown: This action allows you to shut down the system and to stop all services in a proper manner. For systems without a monitor or LCD display, the end of the shutdown process is signaled by an endless series of beeps at intervals of one second.

To shut down Astaro Security Gateway, proceed as follows:

1. Click **Shutdown (Halt) the System Now.**

2. Confirm the warning message.

When asked "Really shut down the system?", click *OK*.

The system is going down for halt.

Depending on your hardware and configuration, this process may take several minutes to complete. Only after the system has completely shut down you should turn off the power. If you turn off the power without the system being shut down properly, the system will check the consistency of its file system during the next booting, meaning that the boot-up process will take much longer than usual. In the worst case, data may have been lost.

The system will beep five times in a row to indicate a successful system start.

Restart: This action will shut down the system completely and reboot. Depending on your hardware and configuration, a complete restart can take several minutes.

To restart Astaro Security Gateway, proceed as follows:

1. Click **Restart (Reboot) the System Now.**

2. Confirm the warning message.

When asked "Really restart the system?", click *OK*.

The system is going down for halt and reboot.

Users

This chapter describes how to configure user accounts, user groups, and external authentication servers of Astaro Security Gateway.

The following topics are included in this chapter:

- Users
- Groups
- Authentication

Users

On the *Users >> Users* tab you can add user accounts to the firewall. In its factory default configuration, Astaro Security Gateway has one administrator called *admin*.

Tip – When you click on a user definition in the *Users* list, you can see all configuration options in which the user definition is used.

When you specify an e-mail address in the *New User* dialog box, an X.509 certificate for this user will be generated simultaneously while creating the user definition, using the e-mail address as the certificate's VPN ID. On the other hand, if no e-mail address is specified, a certificate will be created with the user's *Distinguished Name* (DN) as VPN ID. That way, if a user is authenticated by means of a backend group such as eDirectory, a certificate will be created even if no e-mail address is set in the corresponding backend user object.

Because the VPN ID of each certificate must be unique, each user definition must have a different and unique e-mail address. Creating a user definition with an e-mail address already present in the system will fail. The certificates can be used for various remote access methods supported by Astaro Security Gateway with the exception of PPTP, L2TP over IPSec using preshared keys (PSK), and native IPSec using RSA or PSK.

Users	
 New user ...	
<input type="button" value="Edit"/>   admin <admin@example.com>	
Locally authenticated	
<input type="button" value="Edit"/>   jbots Joe Botts <jbots@example.com>	
Locally authenticated	
<input type="button" value="Edit"/>   jdoe John Doe <jdoe@example.com>	
Locally authenticated	
<input type="button" value="Edit"/>   jsmith <jsmith@example.com>	
Locally authenticated	
<input type="button" value="Find"/>	Display: 25 1-4 of 4

Figure 5.1 Users List

To add a user account, proceed as follows:

1. **On the *Users* tab, click *New User*.**

The *Create New User* dialog box opens.

2. **Make the following settings:**

Username: Enter a descriptive name for this user (e.g. Jdoe).

Real Name: Enter the user's real name (e.g. John Doe).

E-mail Address: Enter the user's primary e-mail address.

Additional E-mail Addresses (optional): Enter additional e-mail addresses of this user. Spam e-mails sent to any of these addresses will be listed in an individual spam report for each e-mail address, which is sent to the primary e-mail address specified above.

Authentication: Select the authentication method. The following methods are available:

- **Local:** Select to authenticate the user locally on the firewall.
- **Remote:** Select to authenticate the user using one of the external authentication methods supported by Astaro Security Gateway. For more information, see *Users >> Authentication*.
- **None:** Select to prevent the user from authentication completely. This is useful, for example, to disable a user temporarily without the need to delete the user definition altogether.

Password: Enter a user password (second time for verification). Only available if you selected *Local* as authentication method. Note that Basic User Authentication does not support umlauts.

Backend Sync: Some basic settings of the user definition such as the real

name or the user's e-mail address can be updated automatically by synchronizing the data with external backend authentication servers (only available if you selected *Remote* as authentication method).

Note – Currently, only data with Active Directory and eDirectory servers can be synchronized.

X.509 Certificate: Once the user definition has been created, you can assign an X.509 certificate for this user when editing the user definition. By default, this is the certificate that was automatically generated upon creating the user definition. However, you can also assign a third-party certificate, which you can upload on the *Remote Access >> Certificate Management >> Certificates* tab.

Use Static Remote Access IP (optional): Select if you want to assign a static IP address for a user gaining remote access instead of assigning a dynamic IP address from an IP address pool. For IPSec users behind a NAT router, for example, it is mandatory to use a static remote access IP address.

Note – The static remote access IP can only be used for remote access through PPTP, L2TP, and IPSec. It cannot be used, however, for remote access through SSL.

Comment (optional): Add a description or other information about the user.

3. Click **Save**.

The new user account appears on the *Users* list.

If you want to make this user a regular administrator having access to the web-based administrative interface WebAdmin, add the user to the group of *SuperAdmins*, which is configured on the *Users >> Groups* tab in WebAdmin.

Note – If you have deleted a user object and want to create a user object with the same name, make sure you have also deleted the certificate associated with this user on the *Remote Access >> Certificate Management >> Certificates* tab. Otherwise you will get an error message stating that an item with that name already exists.

Groups

On the *Users >> Groups* page you can add user groups to the firewall. In its factory default configuration, Astaro Security Gateway has one user group called *SuperAdmins*. If you want to assign administrative privileges to users, that is, granting access to WebAdmin, add them to the group of *SuperAdmins*; this group should not be deleted.

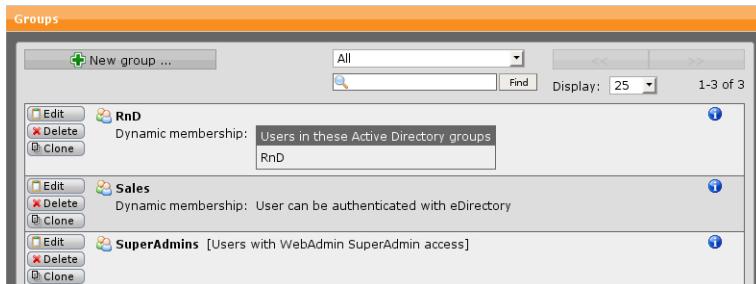


Figure 5.2 Groups List

Tip – When you click on a group definition in the *Groups* list, you can see all configuration options in which the group definition is used.

To add a user group, proceed as follows:

1. On the **User Group Definitions** tab, click **New Group**.
The *Create New Group* dialog box opens.
2. Make the following settings:
 - Group Name:** Enter a descriptive name for this group. Note that this name does not need to correspond to the names of your backend groups.
 - Group Type:** Select the type of the group. You can choose between a group of static members and two group types promoting dynamic membership.
 - **Static Members:** Select the local users who shall become member of this group.
 - **IPSec X509 DN Mask:** Users are dynamically added to an IPSec X509 DN group definition if they have successfully logged in to the firewall

through an IPSec connection and if specific parameters of their distinguished names match the values specified in the *DN Mask* box.

- **Backend Membership:** Users are dynamically added to a group definition if they have been successfully authenticated by one of the supported authentication mechanisms. To proceed, select the appropriate backend authentication type:
 - **Active Directory:** An Active Directory user group of the firewall provides group memberships to members of Active Directory server user groups configured on a Windows network. Enter the name of the Active Directory server groups the user is a member of. For more information, see *Users >> Authentication >> Servers*.
 - **eDirectory:** An eDirectory user group of the firewall provides group memberships to members of eDirectory user groups configured on an eDirectory network. Enter the name of the eDirectory groups the user is a member of. For more information, see *Users >> Authentication >> Servers*.
 - **RADIUS:** Users are automatically added to a RADIUS backend group when they have been successfully authenticated using the RADIUS authentication method.
 - **TACACS+:** Users are automatically added to a TACACS+ backend group when they have been successfully authenticated using the TACACS+ authentication method.
 - **LDAP:** Users are automatically added to an LDAP backend group when they have been successfully authenticated using the LDAP authentication method.

Limit to Backend Group(s) Membership (optional): For all X.500-based directory services you can restrict the membership to various groups present on your backend server if you do not want all users of the selected backend server to be included in this group definition. The group(s) you enter here once selected this option must match a *Common Name* as configured on your backend server. Note that if you select this option for an Active Directory backend, you can omit the *CN=* prefix. If you select this option for an eDirectory backend, you can either use the eDirectory browser that lets you conveniently select the eDirectory groups that should be included in this group definition. However, if you do not use the eDirectory browser, make sure to include the *CN=* prefix when entering eDirectory containers.

Check an LDAP Attribute (optional): If you do not want all users of the selected backend LDAP server to be included in this group definition, you can select this checkbox to restrict the membership to those users matching a certain LDAP attribute present on your backend server. This attribute is then used as an LDAP search filter. For example, you could enter groupMembership as attribute with CN=Sales, O=Example as its value. That way you could include all users belonging to the sales department of your company into the group definition.

Comment (optional): Add a description or other information about the group.

3. Click Save.

The new group appears on the *Group* list.

To either edit or delete a group, click the corresponding buttons.

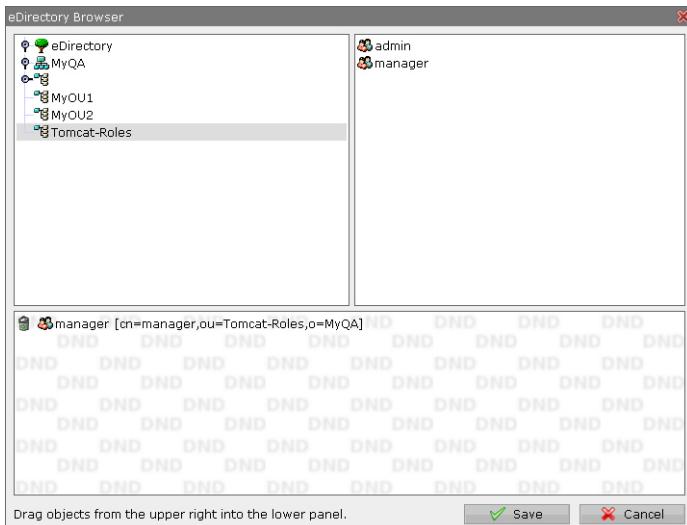


Figure 5.3 eDirectory Browser of Astaro Security Gateway

Authentication

In the menu *Users >> Authentication* databases and backend servers of external user authentication services can be managed. External user authentication allows you to validate user accounts against existing user databases or directory services on other servers of your network. Authentication services currently supported are:

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

Global Settings

The *Global Settings* tab lets you configure basic authentication options. The following options are available:

Create Users Automatically: When this option is selected, Astaro Security Gateway will automatically create a user object whenever an unknown user of a configured backend group successfully authenticates against one of the various authentication services supported by Astaro Security Gateway. For example, if you configure a RADIUS backend group and you select this group in the *Allowed Auditors* box on the *Management >> WebAdmin Settings >> Access Control* tab, Astaro Security Gateway will automatically create a user definition for a RADIUS user who has successfully logged in to WebAdmin.

- **Automatic User Creation for Facilities:** Automatic user creation can be enabled or disabled for specific services. Users are only created for enabled services. This option is not available—and automatic user creation is disabled for all facilities—when the *Create Users Automatically* option is not selected.

Note – This feature does not work for Active Directory *Single Sign-On* (SSO).

Those user objects are also needed to grant access to the User Portal of Astaro Security Gateway. In addition, for all user objects created automatically an SSL

certificate will be generated. Note, however, that automatic user creation will fail in case of an e-mail address conflict, for the user definition to be created automatically must not have configured an e-mail address that is already present on the system. All e-mail addresses must be unique within the system because they are used as identifiers for SSL certificates.

Important Note – Authentication (i.e., the action of determining who a user is) and authorization (i.e., the action of determining what a user is allowed to do) for a user whose user object was created automatically are always done on the remote backend server/directory service. Therefore, automatically created user objects in Astaro Security Gateway are useless if the corresponding backend server is not available or if the user object has been deleted on the remote site.

Note also that except for Active Directory *Single Sign-On* (SSO) Astaro Security Gateway caches user authentication data it has retrieved from a remote authentication server for 300 seconds. For this reason, changes made to the remote user settings will only take effect after the cache has expired.

Authentication Cache

Every time Astaro Security Gateway gets a user request, e.g., http, from a yet unknown user and authentication is required, the Astaro User Authentication (AUA) writes an entry to the authentication cache. Over time, in environments with frequently changing users it can be reasonable to empty the cache from time to time. Also, if you want to force an immediate new authentication for all users. Use the button *Flush Authentication Cache* to empty the authentication cache.

An authentication is valid for 300 seconds. During this time, other authentication requests by the same user are looked up directly in the cache. This technique takes load off backend authentication services like eDirectory.

Note – Flushing the cache does not affect users that are remotely logged on.

Open Live Log: Click the button to see the log of the Astaro User Authentication (AUA) in a new window.

Servers

On the *Users >> Authentication >> Servers* tab, you can create one or more directory servers, such as eDirectory, Active Directory, LDAP, RADIUS, and TACACS+.

eDirectory

Novell eDirectory is an X.500 compatible directory service for centrally managing access to resources on multiple servers and computers within a given network. eDirectory is a hierarchical, object-oriented database that represents all the assets in an organization in a logical tree. Those assets can include people, servers, workstations, applications, printers, services, groups, and so on.

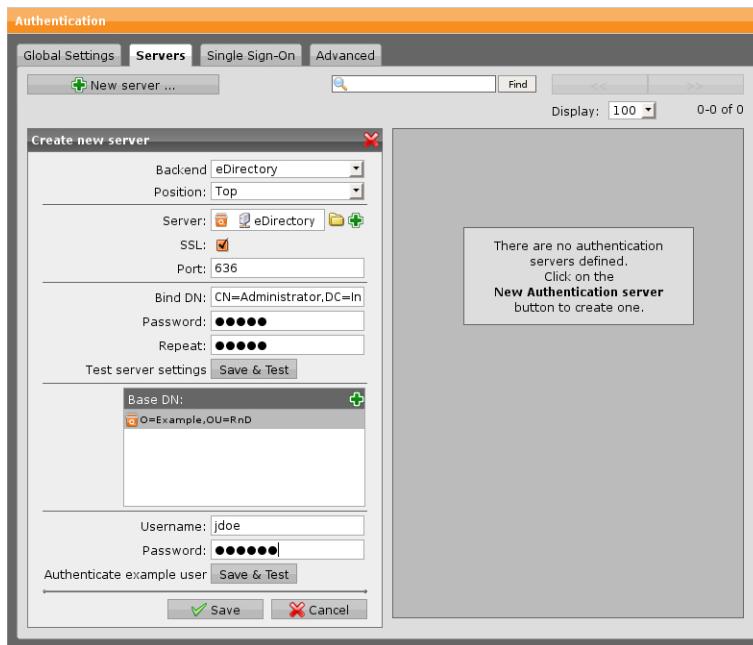


Figure 5.4 Configuring eDirectory User Authentication

To configure eDirectory authentication, proceed as follows:

1. On the Servers tab, click **New Server**.

The dialog window *Create New Server* opens.

2. Make the following settings:

Backend: Select eDirectory as backend directory service.

Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

Server: Select (or add) an eDirectory server.

Use SSL: Select this option to enable SSL data transfer. The **Port** will then change from 389 (LDAP) to 636 (ldaps = LDAP over SSL).

Port: Select the port of the eDirectory server. By default, this is port 389.

Bind DN: The *Distinguished Name* (DN) of the user to bind to the server with. This user is needed if anonymous queries to the eDirectory server are not allowed. Note that the user must have sufficient privileges to obtain all relevant user object information from the eDirectory server in order to authenticate users. eDirectory users, groups, and containers can be specified by the full distinguished name in LDAP notation, using commas as delimiters (e.g., CN=administrator,DC=intranet,DC=example,DC=com).

Password: The password of the bind user (second time for verification).

Test Server Settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings in this tab are correct, and the server is up and accepts connections. The button is only available when you have saved the server settings by clicking the *Apply* button.

Base DN: The starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the base DN must be specified by the full distinguished name (DN) in LDAP notation, using commas as delimiters (e.g., O=Example,OU=RnD). Base DN may be empty. In this case, the Base DN is automatically retrieved from the directory.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

Authenticate Example User: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. Click **Save**.

The server will be displayed in the *Servers* list.

Active Directory

Active Directory (AD) is Microsoft's implementation of a directory service and is a central component of Windows 2000/2003 servers. It stores information about a broad range of resources residing on a network, including users, groups, computers, printers, applications, services, and any type of user-defined objects. As such it provides a means of centrally organizing, managing, and controlling access to these resources.

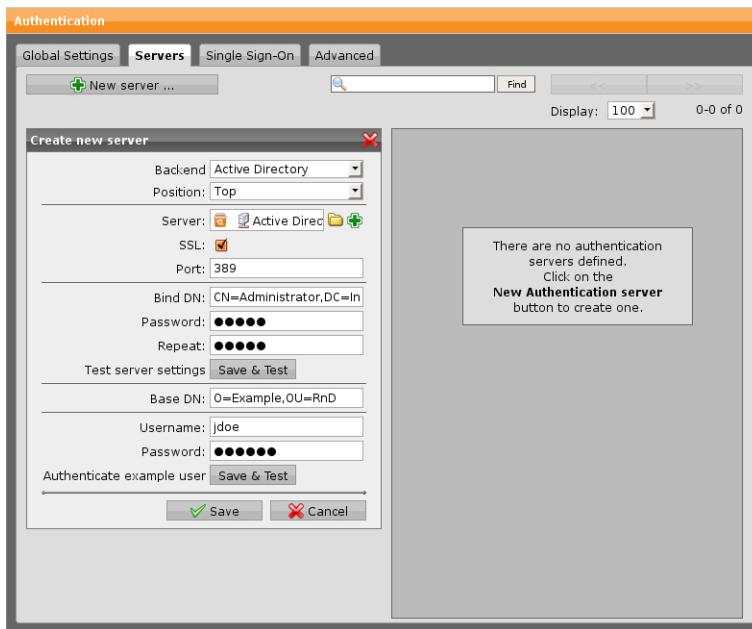


Figure 5.5 Configuring Active Directory User Authentication

The Active Directory authentication method allows you to register Astaro Security Gateway at a Windows domain, thus creating an object for Astaro Security Gateway on the primary *domain controller* (DC). The security system is then able to query user and group information from the domain.

To configure Active Directory authentication, proceed as follows:

1. **On the Servers tab, click New Server.**

The dialog window *Create New Server* opens.

2. **Make the following settings:**

Backend: Select Active Directory as backend directory service.

Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

Server: Select (or add) an Active Directory server.

Use SSL: Select this option to enable SSL data transfer. The *Port* will then change from 389 (LDAP) to 636 (ldaps = LDAP over SSL).

Port: Select the port of the Active Directory server. By default, this is port 389.

Test Server Settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings in this tab are correct, and the server is up and accepts connections. The button is only available when you have saved the server settings by clicking the *Apply* button.

Bind DN: The full *Distinguished Name* (DN) of the user to bind to the server with in LDAP notation. This user is needed as anonymous queries to the Active Directory server are usually not allowed. The bind user must have sufficient privileges to obtain all relevant user object information from the Active Directory server in order to authenticate users; a requirement usually met by the administrator of the domain.

Each DN consists of one or more *Relative Distinguished Names* (RDN) constructed from some attributes of the Active Directory user object and includes its username, the node where it resides, and the top-level DN of the server, all specified in LDAP notation and separated by commas.

- The username must be the name of the user who is able to access the directory and is to be specified by the *CN* designator (e.g., *CN=user*). While using a popular account with domain permissions, such as "admin" is possible, it is highly recommended for best practices that the user not have admin rights, as it is sufficient for them to have read permission on all objects of the subtree starting at the given Base DN.
- The information of the node where the user object resides must include all subnodes between the root node and the user object and is usually comprised of so-called *organizational units* and *common name* components. Organizational units (indicated by the combined folder/book icon in the Microsoft Management Console) are to be specified by the *OU* designator. Note that the order of the nodes is from the lowest to the highest node, that is, the more specific elements come first (e.g., *OU=Management_US,OU=Management*). On the other hand, default Active Directory containers (indicated by a simple folder icon) such as the

pre-defined *Users* node are to be specified using the CN designator (e.g., CN=Users).

- The top-level DN of the server can consist of several domain components, each specified by the DC designator. Note that the domain components are given in the same order as the domain name (for example, if the domain name is example.com, the DN part would be DC=example,DC=com).

An example bind user DN for a user named administrator whose object is stored in the *Users* container in a domain called example.com would look like this: CN=administrator,CN=Users,DC=example,DC=com

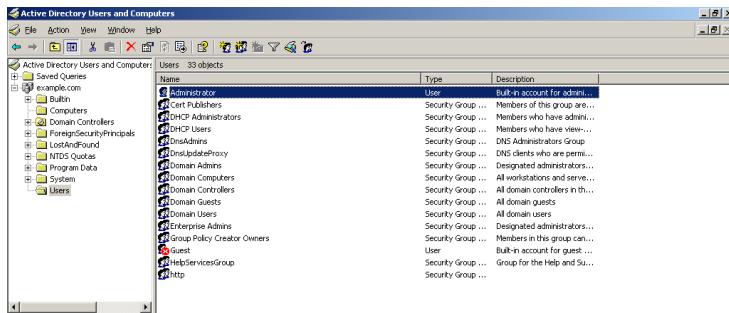


Figure 5.6 Microsoft Management Console (Administrator User Object Highlighted)

Now, suppose you create an organizational unit called *Management* with the subnode *Management_US* and move the administrator user object into it, the DN of the administrator would change to: CN=administrator,OU=Management_US,OU=Management,DC=example,DC=com

Password: The password of the bind user (second time for verification).

Test Server Settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings in this tab are correct, and the server is up and accepts connections. The button is only available when you have saved the server settings by clicking the *Apply* button.

Base DN: The starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the base DN must be specified by the full distinguished name (DN) in LDAP notation, using commas as delimiters (e.g., O=Example,OU=RnD). Base DN may be empty. In this case, the Base DN is automatically retrieved from the directory.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

Authenticate Example User: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. Click **Save**.

The server will be displayed in the *Servers* list.

LDAP

LDAP, an abbreviation for *Lightweight Directory Access Protocol* is a networking protocol for querying and modifying directory services based on the X.500 standard. Astaro Security Gateway uses the LDAP protocol to authenticate users for several of its services, allowing or denying access based on attributes or group memberships configured on the LDAP server.

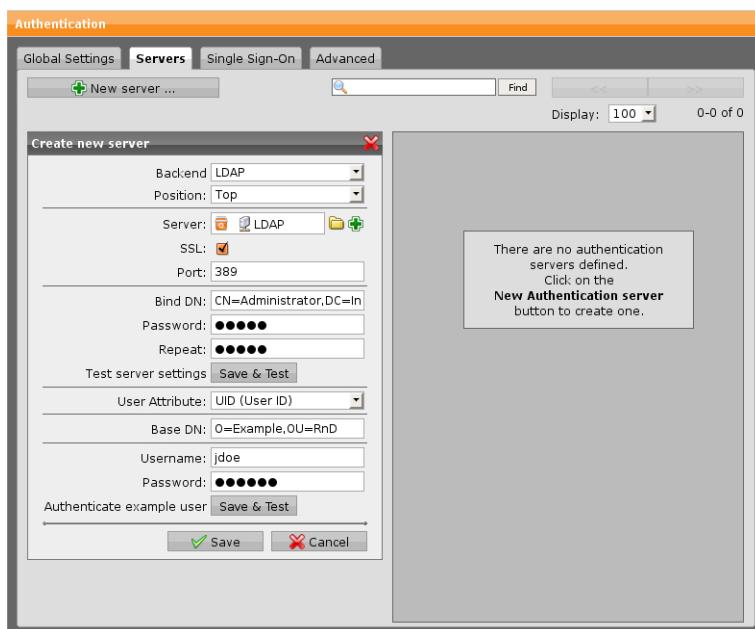


Figure 5.7 Configuring LDAP User Authentication

To configure LDAP authentication, proceed as follows:

1. On the **Servers** tab, click **New Server**.

The dialog window *Create New Server* opens.

2. Make the following settings:

Backend: Select *LDAP* as backend directory service.

Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

Server: Select (or add) an LDAP server.

Use SSL: Select this option to enable SSL data transfer. The *Port* will then change from 389 (LDAP) to 636 (ldaps = LDAP over SSL).

Port: Select the port of the LDAP server. By default, port 389 is selected.

Bind DN: The *Distinguished Name (DN)* of the user to bind to the server with. This user is mandatory. For security reasons, anonymous queries to the LDAP server are not supported. Note that the user must have sufficient privileges to obtain all relevant user object information from the LDAP server in order to authenticate users. LDAP users, groups, and containers can be specified by the full distinguished name in LDAP notation, using commas as delimiters (e.g., CN=administrator,DC=intranet,DC=example,DC=com).

Password: The password of the bind user (second time for verification).

Test Server Settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings in this tab are correct, and the server is up and accepts connections. The button is only available when you have saved the server settings by clicking the *Apply* button.

User Attribute: Select the user attribute that is to be used as the filter for searching the LDAP directory. The user attribute contains the actual login name each user is prompted for, for example by remote access services. The following user attributes can be selected:

- CN (Common Name)
- SN (Surname)
- UID (User ID)

If usernames in your LDAP directory are not stored in any of these forms, select <<Custom>> from the list and enter your custom attribute into the *Custom* field below. Note that this attribute must be configured on your LDAP directory.

Base DN: The starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the base DN must

be specified by the full distinguished name (DN) in LDAP notation, using commas as delimiters (e.g., `O=Example,OU=RnD`). Base DN may be empty. In this case, the Base DN is automatically retrieved from the directory.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

Authenticate Example User: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. Click **Save**.

The server will be displayed in the *Servers* list.

RADIUS

RADIUS, the acronym of *Remote Authentication Dial In User Service* is a widespread protocol for allowing network devices such as routers to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices, such as supported protocols, IP addresses, routing information, and so on. This information constitutes a user profile, which is stored in a file or database on the RADIUS server.

The RADIUS protocol is very flexible, and servers are available for most operating systems. The RADIUS implementation on this security system allows you to configure access rights on the basis of proxies and users. Before you can use RADIUS authentication, you must have a running RADIUS server on the network. As passwords are transmitted in clear text (unencrypted), place the RADIUS server inside the same network as your security system and make sure that the security system and server are on the same switch.

To configure RADIUS authentication, proceed as follows:

1. On the **Servers** tab, click **New Server**.

The dialog window *Create New Server* opens.

2. Make the following settings:

Backend: Select *RADIUS* as backend directory service.

Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

Server: Select (or add) a RADIUS server.

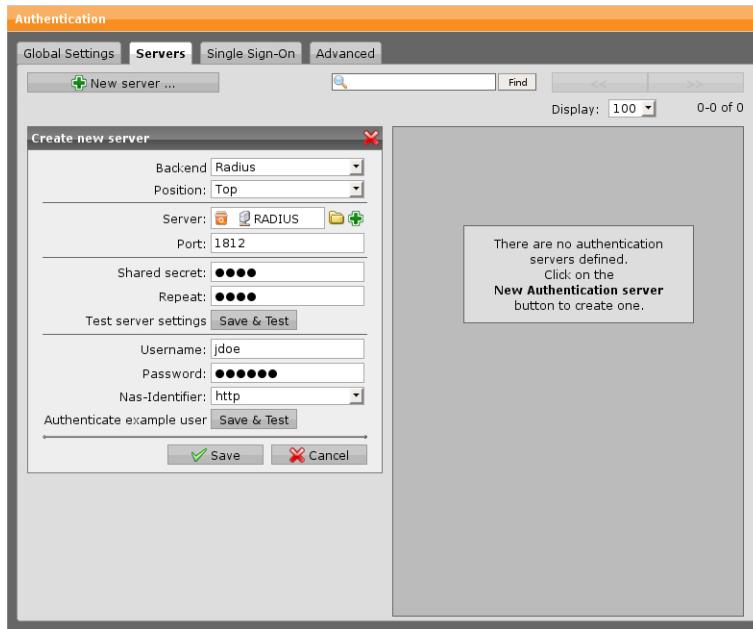


Figure 5.8 Configuring RADIUS User Authentication

Port: Select the port of the RADIUS server. By default, port 1812 is selected.

Shared Secret: The shared secret is a text string that serves as a password between a RADIUS client and a RADIUS server. Enter the shared secret (second time for verification).

Test Server Settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings in this tab are correct, and the server is up and accepts connections. The button is only available when you have saved the server settings by clicking the *Apply* button.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

NAS Identifier: Select the appropriate NAS identifier from the list. For more information see the Note and the table below.

Authenticate Example User: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. Click **Save**.

The server will be displayed in the *Servers* list.

Note – Each user authentication service of Astaro Security Gateway such as PPTP or L2TP querying the RADIUS server sends a different identifier (NAS identifier) to the RADIUS server. For example, the PPTP service sends the NAS identifier pptp to the RADIUS server when trying to authenticate this user. That way, the various services can be differentiated on the RADIUS server, which is useful for authorization purposes, that is, the granting of specific types of service to a user. Below you can find the list of user authentication services and their corresponding NAS identifier.

User Authentication Service	NAS Identifier
SSL VPN	ssl
PPTP	pptp
IPSec	ipsec
L2TP over IPSec	l2tp
SMTP proxy	smtp
User Portal	portal
WebAdmin	webadmin
SOCKS proxy	socks
HTTP/S proxy	http

Table 5.1 RADIUS NAS Identifiers

TACACS

TACACS+ (the acronym of *Terminal Access Controller Access Control System*) is a proprietary protocol by Cisco Systems, Inc. and provides detailed accounting information and administrative control over authentication and authorization processes. Whereas RADIUS combines authentication and authorization in a user profile, TACACS+ separates these operations. Another difference is that TACACS+ utilizes the TCP protocol (port 49) while RADIUS uses the UDP Protocol.

To configure TACACS+ authentication, proceed as follows:

1. **On the Servers tab, click New Server.**

The dialog window *Create New Server* opens.

2. **Make the following settings:**

Backend: Select TACACS+ as backend directory service.

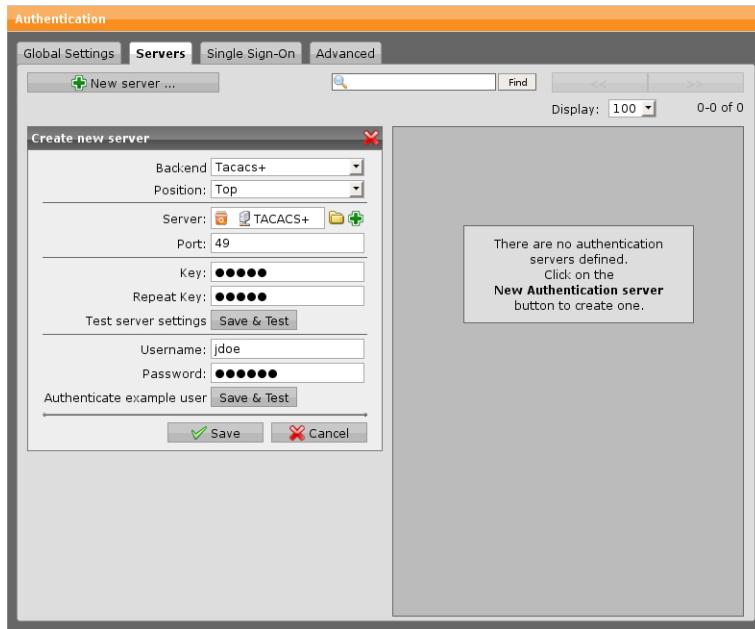


Figure 5.9 Configuring TACACS+ User Authentication

Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

Server: Select (or add) a TACACS+ server.

Port: Select the port of the TACACS+ server. By default, port 49 is selected.

Key: The authentication and encryption key for all TACACS+ communication between Astaro Security Gateway and the TACACS+ server. The value for the key parameter to be entered here should match the one configured on the TACACS+ server. Enter the key (second time for verification).

Test Server Settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings in this tab are correct, and the server is up and accepts connections. The button is only available when you have saved the server settings by clicking the *Apply* button.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

Authenticate Example User: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct,

the server is up and accepting connections, and users can be successfully authenticated.

3. Click **Save**.

The server will be displayed in the *Servers* list.

Single Sign-On

On the *Users >> Authentication >> Single Sign-On* tab you can configure single sign-on functionality for Active Directory and/or eDirectory.

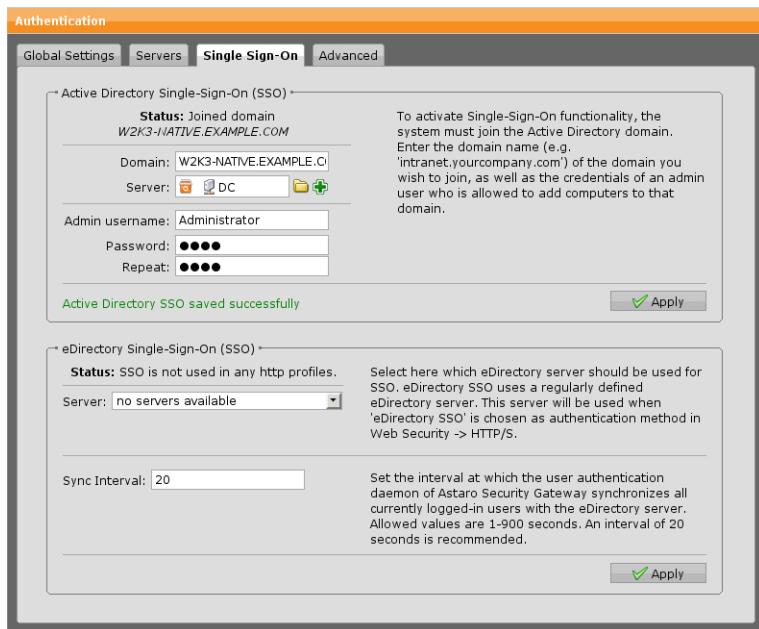


Figure 5.10 Configuring Single Sign-On

Active Directory Single Sign-On (SSO)

Note that the Active Directory SSO facility is currently only used with the HTTP/S proxy to provide single sign-on with browsers that support NTLMv2 or Kerberos authentication.

To activate the single sign-on functionality, the security system must join the Active Directory domain. In order for the domain joining to work, the following prerequisites must be met:

- The time zone on the firewall and the DC must be the same.
- There MUST NOT be a time difference of more than five minutes between the firewall clock and the DC clock.
- The ASG hostname must exist in the AD DNS system.
- The ASG must use the AD DNS as forwarder, or must have a DNS request route for the AD domain which points to the AD DNS server.

To configure Active Directory SSO, do the following:

1. **Create an Active Directory server on the *Servers* tab.**

2. **Make the following settings:**

Domain: Name of the domain (for example `intranet.mycompany.com`).

Server: Select (or add) your Active Directory server.

Admin Username: User with administrative privileges who is allowed to add computers to that domain (usually "Administrator").

Password: The password of the admin user (second time for verification).

3. **Click *Apply*.**

Your settings will be saved.

Note on Kerberos authentication support: In order for opportunistic SSO Kerberos support to work, the clients MUST use the FQDN hostname of the ASG in their proxy settings—using the IP address will not work. NTLMv2 mode is not affected by this requirement, and will automatically be used if it is not met, or if the browser does not support Kerberos authentication.

eDirectory Single Sign-On (SSO)

Here, you can configure SSO for eDirectory. If you have configured *eDirectory SSO* as authentication method in *Web Security >> HTTP/S*, the eDirectory server selected here will be used.

To configure eDirectory SSO, do the following:

1. Create an eDirectory server.

Create an eDirectory server on the *Servers* tab.

2. Select eDirectory server.

Select the eDirectory server from the drop-down list for which you want to enable SSO.

3. Click *Apply*.

Your settings will be saved.

Advanced

Password Complexity

Using this option, you can force the use of strong passwords for administrators or locally registered users having administrative privileges. You can configure password complexity to adhere to the following security requirements:

- Minimum password length, default is eight characters
- Require at least one lowercase character
- Require at least one uppercase character
- Require at least one numeral
- Require at least one non-alphanumeric character

To enable the selected password properties select the *Require complex passwords* checkbox and click *Apply*.

Prefetch Directory Users

Users from eDirectory or Active Directory can be synchronized with the ASG. This will pre-create user objects on the ASG such that these user objects already exist, when the user logs in. The synchronization process can run weekly or daily.

To enable prefetching, make the following settings:

Server: The drop-down list contains servers that have been created on the *Servers* tab. Select a server for which you want to enable prefetching.

Prefetch Interval: Select an interval to prefetch users. To run the synchronization weekly, select the day of the week when synchronization should start. To run the synchronization daily, select *Daily*.

Prefetch Time: Select a time to prefetch users.

eDirectory/Active Directory Groups: To specify which groups should be pre-created, enter the groups here. You can use the integrated LDAP browser to

select these groups.

Enable Backend Sync on Login (optional): Select this option if user information shall be fetched from the directory during login of an yet unknown user.

Click Apply.

Your settings will be saved.

Prefetch Now: Click this button to start prefetching immediately.

Open: Click this button to open the prefetch live log.

Definitions

This chapter describes how to configure network, service, and time event definitions used throughout Astaro Security Gateway. The *Definitions Overview* page in WebAdmin shows the number of network definitions according to type as well as the numbers of service definitions according to protocol type.

The pages of the *Definitions* menu allow you to define networks and services that can be used in all other configuration menus in one central place. This allows you to work with the names you define rather than struggling with IP addresses, ports, and network masks. Another benefit of definitions is that you can group individual networks and services together and configure them all at once. If, for example, you assign certain settings to these groups at a later time, these settings will apply to all networks and services contained therein.

The following topics are included in this chapter:

- Networks
- Services
- Time Events

Networks

The *Definitions >> Networks* page is the central place for defining hosts, networks, and network groups on the security system. The definitions created here can be used on many other WebAdmin configuration menus.

Tip – When you click on the info icon of a network definition in the Networks list, you can see all configuration options in which the network definition is used.

The network table also contains static networks, which were automatically created by the system and which can neither be edited nor deleted:

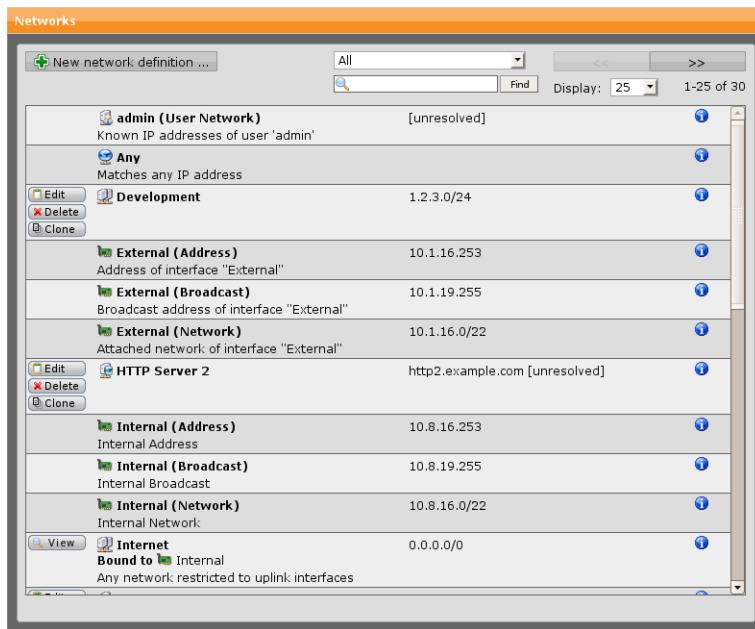


Figure 6.1 Network Definition List

- **Interface Address:** A definition of this type will be added for each network interface. It contains the current IP address of the interface. Its name consists of the interface name with "(Address)" appended to it.
- **Interface Broadcast Address:** A definition of this type will be added for each Ethernet-type network interface. It contains the current IPv4 broadcast address of the interface. Its name consists of the interface name with "(Broadcast)" appended to it.
- **Interface Network Address:** A definition of this type will be added for each Ethernet-type network interface. It contains the current IPv4 network of the interface. Its name consists of the interface name with "(Network)" appended to it.
- **Internet:** A network definition bound to the interface which serves as default gateway. Making use of it in your configuration should make the configuration process easier. With *Uplink Balancing* enabled, *Internet* is bound to *uplink interfaces*.

To create a network definition, proceed as follows:

1. On the Networks tab, click **New Network Definition**.

The Create New Network Definition dialog box opens.

2. Make the following settings:

(Note that further parameters of the network definition will be displayed depending on the selected definition type.)

Name: Enter a descriptive name for this definition.

Type: Select the network definition type. The following types are available:

- **Host:** A single IPv4 address. Provide the following information:
 - **Address:** The IP address of the host (note that you cannot enter the IP address of an configured interface).
 - **Interface (optional):** You can bind the network definition to a certain interface, so that connections to the definition will only be established via this interface.
 - **Comment (optional):** Add a description or other information about this host.
- **DNS Host:** A DNS hostname, dynamically resolved by the system to produce an IP address. DNS hosts are useful when working with dynamic IP endpoints. The system will re-resolve these definitions periodically according to the TTL (Time To Live) values and update the definition with the new IP address (if any). Provide the following information:
 - **Interface (optional):** You can bind the network definition to a certain interface, so that connections to the definition will only be established via this interface.
 - **Hostname:** The hostname you want to resolve.
 - **Comment (optional):** Add a description or other information about this DNS host.
- **DNS Group:** Similar to DNS host, but can cope with multiple RRs (Resource Records) in DNS for a single hostname. It is useful for defining packet filter rules and for exception lists in transparent proxies.
- **Network:** A standard IPv4 network, consisting of a network address and a netmask. Provide the following information:

- **Address:** The network address of the network (note that you cannot enter the IP address of a configured interface).
 - **Interface (optional):** You can bind the network definition to a certain interface, so that connections to the definition will only be established via this interface.
 - **Netmask:** The bitmask used to tell how many bits in an octet(s) identify the subnetwork, and how many bits provide room for host addresses.
 - **Comment (optional):** Add a description or other information about this network.
- **Multicast Group:** A network that comprises a defined multicast network range.
 - **Address:** The network address of the multicast network, which must be in the range 224.0.0.0 to 239.255.255.255.
 - **Interface (optional):** You can bind the network definition to a certain interface, so that connections to the definition will only be established via this interface.
 - **Netmask:** The bitmask used to tell how many bits in an octet(s) identify the subnetwork, and how many bits provide room for host addresses.
 - **Comment (optional):** Add a description or other information about this network.
 - **Network Group:** A container that includes a list of other network definitions. You can use them to bundle networks and hosts for better readability of your configuration. Once you have selected *Network Group*, the *Members* box appears where you can add the group members.
 - **Availability Group:** A group of hosts and/or DNS hosts sorted by priority. Alive status of all hosts is checked with ICMP pings at a specified interval. The host with the highest priority and an alive status is used in configuration.

- **Members:** Add the group members.
- **Check Interval:** Enter a time interval in seconds at which the hosts are ping-checked.

3. Click Save.

The new definition appears on the network definition list.

To either edit or delete a network definition, click the corresponding buttons.

Services

On the *Definitions >> Services* page you can centrally define and manage services and service groups. Services are definitions of certain types of network traffic and combine information about a protocol such as TCP or UDP as well as protocol-related options such as port numbers. You can use services to determine the types of traffic accepted or denied by the firewall.

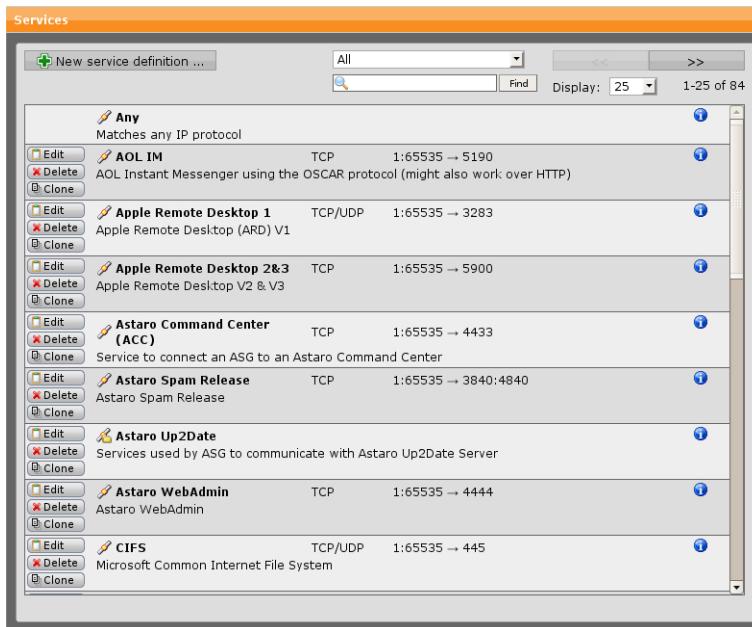


Figure 6.2 Service Definitions List

Tip – When you click on the info icon of a service definition in the *Services* list, you can see all configuration options in which the service definition is used.

To create a service definition, proceed as follows:

1. **On the *Definitions* >> *Services* tab, click *New Service Definition*.**

The *Create New Service Definition* dialog box opens.

2. **Make the following settings:**

(Note that further parameters of the network definition will be displayed depending on the selected definition type.)

Name: Enter a descriptive name for this definition.

Type of Definition: Select the service type. The following types are available:

- **TCP:** Transmission Control Protocol (TCP) connections use port numbers ranging from 0 to 65535. Lost packets can be recognized through TCP and be requested again. In a TCP connection, the receiver notifies the sender when a data packet was successfully received (connection related protocol). TCP sessions begin with a three way handshake and connections are closed at the end of the session. Provide the following information:

- **Destination Port:** Enter the destination port either as single port number (e.g., 80) or as a range (e.g., 1024:64000), using a colon as delimiter.
- **Source Port:** Enter the source port either as single port number (e.g., 80) or as a range (e.g., 1024:64000), using a colon as delimiter.

- **UDP:** The *User Datagram Protocol* (UDP) uses port numbers between 0 and 65535 and is a stateless protocol. Because it does not keep state, UDP is faster than TCP, especially when sending small amounts of data. This statelessness, however, also means that UDP cannot recognize when packets are lost or dropped. The receiving computer does not signal the sender when receiving a data packet. When you have selected *UDP*, the same configuration options can be edited as for TCP.

- **TCP/UDP:** A combination of TCP and UDP appropriate for application protocols that use both subprotocols such as DNS. When you have selected *TCP/UDP*, the same configuration options can be edited as for TCP or UDP.

- **ICMP:** The *Internet Control Message Protocol* (ICMP) is chiefly used to send error messages, indicating, for example, that a requested service is

not available or that a host or router could not be reached. Once you have opted for *ICMP*, select the ICMP code/type.

- **IP:** The *Internet Protocol* (IP) is a network and transport protocol used for exchanging data over the Internet. Once you have selected *IP*, provide the number of the protocol to be encapsulated within IP, for example 121 (representing the SMP protocol).
- **ESP:** The *Encapsulating Security Payload* (ESP) is a part of the IPSec tunneling protocol suite that provides encryption services for tunneled data via VPN. Once you have selected *ESP* or *AH*, provide the *Security Parameters Index* (SPI), which identifies the security parameters in combination with the IP address. You can either enter a value between 256 and 4,294,967,296 or keep the default setting given as the range from 256 to 4,294,967,296 (using a colon as delimiter), especially when using automatic IPSec key exchange. Note that the numbers 1–255 are reserved by the *Internet Assigned Numbers Authority* (IANA).
- **AH:** The *Authentication Header* (AH) is a part of the IPSec tunnelling protocol suite and sits between the IP header and datagram payload to maintain information integrity, but not secrecy.
- **Group:** A container that includes a list of other service definitions. You can use them to bundle service definitions for better readability of your configuration. Once you have selected *Group*, the *Members* dialog box opens where you can add group members (i.e., other service definitions).

Comment (optional): Add a description or other information about the service definition.

3. Click **Save**.

The new definition appears on the service definition list.

To either edit or delete a network definition, click the corresponding buttons.

Note – The type of definition cannot be changed afterwards. If you want to change the type of definition, you must delete the service definition and create a new one with the desired settings.

Time Events

On the *Definitions >> Time Events* page you can define single or recurring time slots that can in turn be used to limit packet filter rules or content filter profile assignments to specific time ranges.

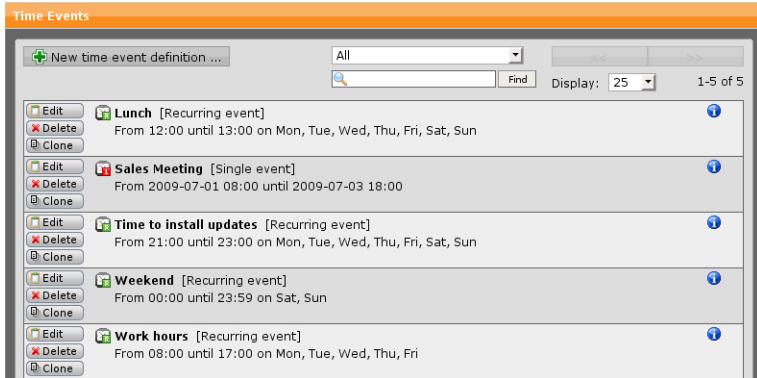


Figure 6.3 Time Events Definitions List

Tip – When you click on the info icon of a time event definition in the *Time Events* list, you can see all configuration options in which the time event definition is used.

To create a time event definition, proceed as follows:

1. On the **Time Event Definitions** tab, click **New Time Event Definition**.
The *Create New Time Event Definition* dialog box opens.
2. Make the following settings:
 - Name:** Enter a descriptive name for this time event.
 - Type:** Select the time event definition type. The following types are available:
 - o **Recurring Event:** These events will be repeated periodically. You can select the start time, the end time, and the weekdays on which the time

event definition should be applied. Start and stop dates cannot be selected for this type.

- **Single Event:** These events will only take place once. You can both select a start date/time and an end date/time. As these definitions do not recur, the option *Weekdays* cannot be selected for this type.
- **Comment (optional):** Add a description or other information about the time event.

3. Click **Save**.

The new time event definition appears on the time event definition list.

To either edit or delete a time event definition, click the corresponding buttons.

Note – You can only delete time event definitions that are not used in either a packet filter rule or within a *Web Security >> HTTP/S Profiles >> Filter Assignment*.

Network

This chapter describes how to configure Astaro Security Gateway to operate in your network. The *Network Statistics* page in WebAdmin provides an overview of today's top ten accounting services, top source hosts, and concurrent connections. Each of the sections contains a *Details* link. Clicking the link redirects you to the respective *Reporting* section of WebAdmin, where you can find more statistical information.

The following topics are included in this chapter:

- Interfaces
- Bridging
- Static Routing
- Dynamic Routing (OSPF)
- Quality of Service (QoS)
- Multicast Routing (PIM-SM)
- Uplink Monitoring

Interfaces

A firewall requires at least two network interface cards to connect an internal network (LAN) to an external one (e.g., the Internet) in a secure fashion. In the following examples, the network card `eth0` is always the interface connected to the internal network. Network card `eth1` is the interface connected to the external network (for example, to the Internet). These interfaces are also called the trusted and untrusted interfaces, respectively.

Network cards are automatically recognized during the installation. With the Software Appliance, if new network cards are added later, a new installation will be necessary. To reinstall the system, simply make a backup of your configuration, install the software, and restore your backup.

The firewall must be the only point of contact between internal and external networks. All data must pass through the security system. We strongly recommend against connecting both internal and external interfaces to one hub or switch, except if the switch is configured as a VLAN switch. There might be wrong ARP resolutions (Address Resolution Protocol), also known as "ARP clash", which cannot be administered by all operating systems (for example, such as those from Microsoft). Therefore, one physical network segment has to be used for each firewall network interface.

The *Interfaces* menu allows you to configure and manage all network cards installed on the security system and also all interfaces with the external network (Internet) and interfaces to the internal networks (LAN, DMZ).

Note – While planning your network topology and configuring the security system, take care to note which interface is connected to which network. In most configurations, the network interface with SysID `eth1` is chosen as the connection to the external network. In order to install the high-availability (HA) failover, the selected network cards on both systems must have the same SysID. Installing the HA failover is described in more detail on page [High-Availability](#).

The following sections explain how to use the tabs *Interfaces*, *Additional Addresses*, *Link Aggregation*, *Uplink Balancing*, *Multipath Rules*, and *Hardware* to manage the various interface types.

Interfaces

On the *Interfaces* you can configure network cards and virtual interfaces. The list shows the already defined interfaces with their symbolic name, hardware device, and current addresses. The interface status is also displayed. By clicking the status icon, you can activate and deactivate interfaces.

Tip – When you click the info icon of an interface definition in the *Interfaces* list, you can see all configuration options in which the interface definition is used.

Newly added interfaces may show up as *Down* while they are in the process of being set up. You can select to edit and delete interfaces by clicking the respective buttons.

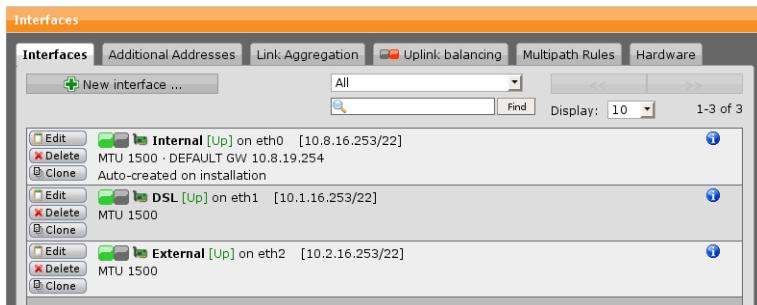


Figure 7.1 Configuring Interfaces

Automatic Interface Network Definitions

Each interface on your firewall has a symbolic name and a hardware device assigned to it. The symbolic name is used when you reference an interface in other configuration settings. For each interface, a matching set of network definitions is automatically created by the firewall:

- A definition containing the current IP address of the interface, its name consisting of the interface name and the *(Address)* suffix.
- A definition containing the network attached to the interface, its name consisting of the interface name and the *(Network)* suffix. This definition is not created for *Point-to-Point* (PPP) type interfaces.
- A definition containing the broadcast address of the interface, its name consisting of the interface name and the *(Broadcast)* suffix. This definition is not created for *Point-to-Point* (PPP) type interfaces.

When the interface uses a dynamic address allocation scheme (such as DHCP or remote assignment), these definitions are automatically updated. All settings referring to these definitions, for example packet filter and NAT rules, will also automatically be updated with the changed addresses. One interface with the symbolic name *Internal* is already predefined. It is the management interface and will typically be used as the "internal" firewall interface. If you want to rename it, you should do so right after the installation.

Interface Types

The following list shows which interface types can be added to the firewall, and what type of hardware is needed to support them:

Ethernet Standard: This is a normal Ethernet interface, with 10, 100, or 1000 Mbit/s bandwidth.

Ethernet VLAN: VLAN (Virtual LAN) is a method to have multiple layer-2 separated network segments on a single hardware interface. Every segment is identified by a "tag", which is just an integer number. When you add a VLAN interface, you will create a "hardware" device that can be used to add additional interfaces (aliases), too. PPPoE and PPPoA devices cannot be run over VLAN virtual hardware.

Cable Modem (DHCP): This is a standard Ethernet interface with DHCP.

DSL (PPPoE): PPP over Ethernet. A DSL PPPoE device lets you attach your firewall to *PPP-over-Ethernet* compatible DSL lines. These devices require a dedicated Ethernet connection (they cannot co-exist with other interfaces on the same hardware). You must attach a DSL modem to the interfaces network segment. The network parameters for these device types can be assigned by the remote station (typically, your ISP). In addition, you need to enter username and password for your ISP account.

DSL (PPPoA/PPTP): PPP over ATM. A DSL PPPoA device lets you attach your firewall to *PPP-over-ATM* compatible DSL lines. These devices use the PPT protocol to tunnel IP packets. They require a dedicated Ethernet connection (they cannot co-exist with other interfaces on the same hardware). You must attach a DSL modem to the interfaces network segment. The network parameters for these device types can be assigned by the remote station (typically, your ISP). In addition, you need to enter username and password for your ISP account. You also need to enter the IP address of your modem. This address is usually hardwired in the modem and cannot be changed. To communicate with the modem, you have to enter a NIC IP address and netmask. The modem's IP address must be inside the network defined by these parameters. The *Ping Address* must be a host on the other side of the PPTP link that responds to ICMP ping requests. You can try to use the DNS server of your ISP. If this address cannot be pinged, the connection is assumed to be dead, and will be reinitiated.

Modem (PPP): This type of interface lets you connect the security system to the Internet through a PPP modem. For the configuration you need a serial interface and an external modem on the security system. And you also need the DSL access data including password. You will get these data from your provider.

Ethernet Standard

To configure a network card for a standard Ethernet connection to an internal or external network, you must configure the network card with an IP address and netmask.

To configure a standard Ethernet interface, proceed as follows:

1. **On the *Interfaces* tab, click *New Interface*.**

The *Create New Interface* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for the interface.

Type: Select *Ethernet Standard* from the type list.

Hardware: Select an interface from the *Hardware* list.

Tip – For an external connection (e.g., to the Internet) choose the network card with SysID eth1. Please note that one network card cannot be used as both an *Ethernet Standard* interface and a PPP over Ethernet (PPPoE DSL) or PPPTP over Ethernet (PPPoA DSL) connection simultaneously.

Address: Enter the IP address of the interface.

Netmask: Select a network mask.

Default GW (optional): If you want to use a statically defined default gateway, select the checkbox *Default GW*.

Default GW IP (optional): Enter the IP address of the default gateway.

Proxy ARP: To enable the function, select the checkbox. By default, the *Proxy ARP* function is disabled (Off).

This option is available on broadcast-type interfaces. When you switch it on, the firewall will "attract" traffic on that interface for hosts "behind" it and pass it on. It will do that for all hosts that it has a direct interface route for. This allows you to build "transparent" network bridging while still doing firewalling. Another use for this feature is when your ISP's router just puts your "official" network on its Ethernet interface (does not use a host route).

MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. By default, an MTU of 1500 bytes is set for the *Ethernet Standard* interface type. An MTU

size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface).

Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Comment (optional): Add a description or other information about the interface.

3. Click **Save**.

The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (status icon is red).

4. Enable the interface.

Click the status icon to activate the interface.

The interface is now enabled (status icon is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

Ethernet VLAN

In order to connect the security system to the virtual LANs, the system requires a network card with a tag-capable driver. A tag is a 4-byte header attached to packets as part of the Ethernet header. The tag contains the number of the VLAN that the packet should be sent to: the VLAN number is a 12-bit number, allowing up to 4095 virtual LANs. In WebAdmin this number is referred to as the *VLAN tag*.

Note – In order to configure an Ethernet Virtual LAN interface, you will need a network card with a tag-capable driver. The *Hardware Compatibility List*

(HCL) can be found at Astaro's knowledgebase¹⁷. Use "HCL" as search term to find the corresponding page.

To configure an Ethernet VLAN interface, proceed as follows:

1. **On the *Interfaces* tab, click *New Interface*.**

The *Create New Interface* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for the interface.

Type: Select *Ethernet VLAN* from the type list.

Hardware: Select an interface from the hardware list.

VLAN Tag: Enter the VLAN tag to use for this interface.

Address: Enter the IP address of the interface.

Netmask: Select a network mask.

Default GW (optional): If you want to use a statically defined default gateway, select the checkbox *Default GW*.

Default GW IP (optional): Enter the IP address of the default gateway.

MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. By default, an MTU of 1500 bytes is set for the *Ethernet VLAN* interface type. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface).

Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Comment (optional): Add a description or other information about the interface.

3. **Click *Save*.**

The system will now check the settings for validity. After a successful check

¹⁷ <http://www.astaro.com/kb/>

the new interface will appear in the interface list. The interface is not yet enabled (status icon is red).

4. Enable the interface.

Click the status icon to activate the interface.

The interface is now enabled (status icon is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

Cable Modem (DHCP)

To configure a *Cable Modem (DHCP)* interface, proceed as follows:

1. On the *Interfaces* tab, click **New Interface**.

The *Create New Interface* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for the interface.

Type: Select *Cable Modem (DHCP)* from the type list.

Hardware: Select an interface from the hardware list.

Tip – For an external connection (e.g., to the Internet) choose the network card with SysID eth1. Please note that one network card cannot be used as both a *Cable Modem (DHCP)* and a *PPP over Ethernet* (PPPoE-DSL) or *PPPTP over Ethernet* (PPPoA-DSL) connection simultaneously.

Default GW (optional): If you want to use a statically defined default gateway, select the checkbox *Default GW*.

Default GW IP (optional): Enter the IP address of the default gateway.

Proxy ARP: To enable the function, select the checkbox. By default, the *Proxy ARP* function is disabled (Off).

This option is available on broadcast-type interfaces (currently *Ethernet Standard* only). When you switch it on, the firewall will "attract" traffic on that interface for hosts "behind" it and pass it on. It will do that for all hosts that it has a direct interface route for. This allows you to build "transparent" network bridging while still doing firewalling. Another use

for this feature is when your ISP's router just puts your "official" network on its Ethernet interface (does not use a host route).

MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. By default, an MTU of 1500 bytes is set for the *Cable Modem* interface type. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface).

Hostname (optional): If your ISP requests that you submit a specific hostname with your DHCP request, you can enter it in this field. However, only add it if it is a requirement.

Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Comment (optional): Add a description or other information about the interface.

3. Click **Save**.

The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (status icon is red).

4. Enable the interface.

Click the status icon to activate the interface.

The interface is now enabled (status icon is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

DSL (PPPoE)

The configuration will require the DSL connection information, including user-name and password, provided by your Internet Service Provider (ISP). VDSL is also supported by this interface type.

Note – The installation and specific settings required for DSL connections are described in the *DSL Network Guide*. Also note that, once the DSL connection is activated, the security system will be connected to your ISP 24 hours a day. You should therefore ensure that your ISP bills on a flat-rate or bandwidth-based system rather than based on connection time. The *DSL Network Guide* is available at Astaro's knowledgebase¹⁸.

To configure a DSL (PPPoE) interface, proceed as follows:

1. On the **Interfaces tab**, click **New Interface**.

The *Create New Interface* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for the interface.

Type: Select DSL (PPPoE) from the type list.

Hardware: Select an interface from the hardware list.

VDSL: Select this checkbox if and only if your connection is a VDSL connection. The *MTU Size* changes to 1476.

Default GW (optional): If you want to use a statically defined default gateway, select the checkbox *Default GW*.

Default GW IP (optional): Enter the IP address of the default gateway.

Username: Enter the username, provided by your ISP.

Password: Enter the password, provided by your ISP.

Daily Reconnect: You can set the daily reconnect from *Never* to any time.

Reconnect Delay: By default, delay is set to *5 Seconds*. If your ISP demands a longer delay you can set it to *One Minute* or *Fifteen Minutes*.

MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. By default, an MTU of 1492 bytes is set for the *DSL (PPPoE)* interface type. An MTU size greater than 1500 bytes must be supported by the network operator and

¹⁸ <http://www.astaro.com/kb/>

the network card (e.g., Gigabit interface).

Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Comment (optional): Add a description or other information about the interface.

3. Click **Save**.

The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (status icon is red).

4. Enable the interface.

Click the status icon to activate the interface.

The interface is now enabled (status icon is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

DSL (PPPoA/PPTP)

To configure a connection using the *PPP over ATM Protocol* (PPPoA), you will need an unused Ethernet interface on the security system as well as an external ADSL modem with an Ethernet port. The connection to the Internet proceeds through two separate connections. Between the security system and the ADSL modem, a connection using the *PPTP over Ethernet Protocol* is established. The ADSL modem is, in turn, connected to the ISP using the *PPP over ATM Dialing Protocol*.

The configuration will require the DSL connection information, including user-name and password, provided by your Internet Service Provider (ISP).

Note – The installation and specific settings required for DSL connections are described in the *DSL Network Guide*. Also note that, once the DSL connection is activated, the security system will be connected to your ISP 24 hours a day. You should therefore ensure that your ISP bills on a flat-rate or bandwidth-based system rather than based on connection time. The *DSL Network Guide* is available at Astaro's knowledgebase¹⁹.

To configure a DSL (PPPoA) interface, proceed as follows:

1. **On the *the Interfaces* tab, click *New Interface*.**

The *Create New Interface* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for the interface.

Type: Select *DSL (PPPoA)* from the type list.

Hardware: Select an interface from the hardware list.

Default GW (optional): If you want to use the default gateway of your provider, click the checkbox.

Modem IP: Enter the IP address of your ADSL modem here. This address will usually be provided by your ISP or the modem hardware and cannot be changed. Example: 10.0.0.138 (with AonSpeed).

NIC Address: Enter the IP address of the network card on the security system which is attached to the modem here. This address must be in the same subnet as the modem. Example: 10.0.0.140 (with AonSpeed).

NIC Netmask: Enter the network mask to use here.

Example: 255.255.255.0 (with AonSpeed).

Ping Address: Enter the IP address of a host on the Internet that responds to ICMP ping requests. In order to test the connection between the security system and the external network, you have to enter an IP address of a host on the other side of the PPTP link. You can try to use the DNS server of your ISP. The security system will send ping requests to this host: if no answer is received, the connection will be broken.

Username: Enter the username, provided by your ISP.

Password Enter the password, provided by your ISP.

Daily Reconnect: You can set the daily reconnect from Never to any time.

MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default.

¹⁹ <http://www.astaro.com/kb/>

Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. By default, an MTU of 1492 bytes is set for the *DSL (PPPoA)* interface type. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface).

Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Comment (optional): Add a description or other information about the interface.

3. Click **Save**.

The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (status icon is red).

4. Enable the interface.

Click the status icon to activate the interface.

The interface is now enabled (status icon is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

Modem (PPP)

For the configuration you need a serial interface and an external PPP modem on the security system. And you also need the DSL access data including username and password. You will get these data from your Internet Service Provider (ISP).

To configure a *Modem (PPP)* interface, proceed as follows:

1. On the **Interfaces** tab, click **New Interface**.

The *Create New Interface* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for the interface.

Type: Select *Modem (PPP)* from the type list.

Hardware: Select an interface from the hardware list.

Default GW (optional): If you want to use the default gateway of your provider, click the checkbox.

Username: Enter the username, provided by your ISP.

Password Enter the password, provided by your ISP.

Line Speed: Set the speed in bits per seconds for the connection between the security system and the modem. Common values are 57,600 Bits/s and 115,200 Bits/s.

Flow Control: Select the method to control the data flow.

If the data is transferred via the serial connection it might happen that the system cannot process incoming data fast enough. To ensure that no data is lost, this method of controlling the data flow becomes necessary. With the serial connection two methods are available:

- *Hardware signals*
- *Software signals*

Since in a PPP connection all eight bits are used for the data transfer line and the transferred data contains the bytes of the command signs *Control S* and *Control Q*, we recommend keeping the default setting *Hardware* and using a serial connection cable.

Init String: Enter the string to initialize the modem. Remember that it might become necessary to adjust the init string to the modem. In this case, the init string can be gathered from the associated modem manual. If you do not have the required documentation available, keep the default setting *ATZ*.

Dial String: Enter ATDT plus the phone number. Example: ATDT5551230

Reset String: Enter the reset string for the modem. Keep in mind that it might be necessary to adjust the reset string to the modem. In this case you can gather it from the associated modem manual. If you do not have the required documentation available, keep the default setting *ATZ*.

MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. By default, an

MTU of 1492 bytes is set for the *Modem (PPP)* interface type. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface).

Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either Mbps or kbps. Select the appropriate unit from the drop-down list.

Comment (optional): Add a description or other information about the interface.

3. Click **Save**.

The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (status icon is red).

4. Enable the interface.

Click the status icon to activate the interface.

The interface is now enabled (status icon is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

Additional Addresses

One network card can be configured with additional IP addresses (also called *aliases*). This function allows you to manage multiple logical networks on one physical network card. It can also be used to assign further addresses to a security system running NAT (Network Address Translation).

To configure additional addresses on standard Ethernet interfaces, proceed as follows:

1. On the **Additional Addresses** tab, click **New Additional Address**.

The Create New Additional Address dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for the new additional address.

On Interface: Select an interface from the drop-down list to which the address is to be assigned.

Address: Enter the IP address of the interface.

Netmask: Select a netmask from the drop-down list.

Comment (optional): Add a description or other information about the additional address.

3. Click **Save**.

The system will now check the settings for validity. After a successful check the new additional address will appear in the list. The interface is not yet enabled (status icon is red).

4. Enable the additional address.

Click the status icon to activate the additional address.

The additional address is now enabled (status icon is green). The additional address might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the additional address is fully operable.

To either edit or delete an additional address, click the corresponding buttons.

Link Aggregation

Link aggregation, which is also known as "port trunking" or "NIC bonding", allows you to aggregate multiple Ethernet network ports into one virtual interface. The aggregated ports appear as a single IP address to your system. Link aggregation is useful to increase the link speed beyond the speed of any one single NIC or to provide basic failover and fault tolerance by redundancy in the event any port or switch fails. All traffic that was being routed over the failed port or switch is automatically re-routed to use one of the remaining ports or switches. This failover is completely transparent to the system using the connection.

Note – In a high-availability environment, Ethernet connections can even be on different HA units.

You can define up to four different link aggregation groups with a maximum of four Ethernet interfaces per group. You need at least two free network interface cards for one link aggregation group, one of which must be unconfigured.

To create a link aggregation group (LAG), proceed as follows:

1. For each LAG, select a configured interface.

From the *Convert Interface* list, select the interfaces you want to convert into a link aggregation group.

2. For each LAG, select an unconfigured interface.

Select the checkbox for each unconfigured interface you want to add to the link aggregation group.

3. Enable the LAG.

Activate a group by clicking the button *Enable this group*.

Once the link aggregation group has been configured, a new LAG interface (e.g., 1ag0) becomes available for selection if you are going to create an interface definition on the *Network >> Interfaces* tab. On top of the bonding interface you can create one of the following:

- Ethernet Standard
- Ethernet VLAN
- Cable Modem (DHCP)
- Alias interfaces

To disable a LAG, clear the checkboxes of the interfaces that make up the LAG and click *Update this Group*. The status of the LAG interface is shown on the *Support >> Advanced >> Interfaces Table* tab.

Uplink Balancing

With the upload balancing function you can combine more than one Internet uplink, either for having backup uplinks available or for using load balancing among multiple uplinks. Combining up to eight different uplinks is supported.

To use uplink balancing, proceed as follows:

1. Enable uplink balancing.

You can either click the status icon or the *Enable* button.

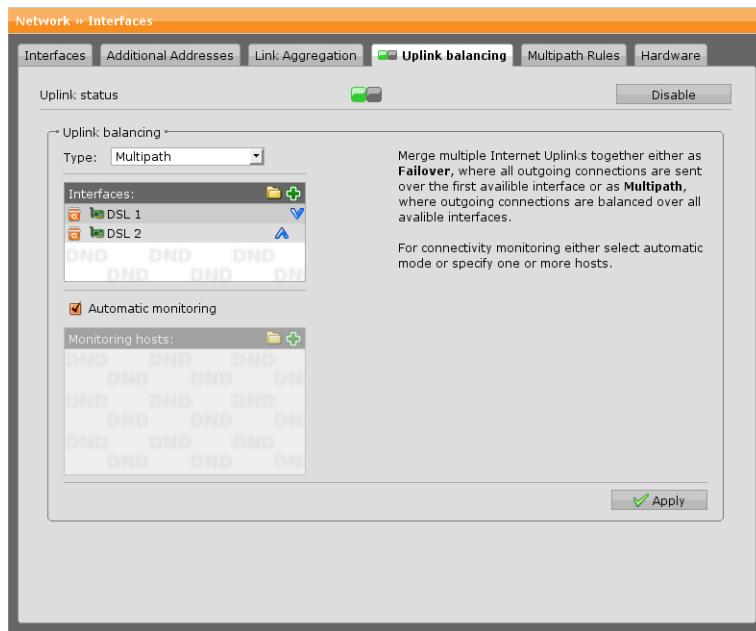


Figure 7.2 Configuring Uplink Balancing

The status icon turns amber and the *Uplink Balancing* area becomes editable.

2. Select the balancing type.

From the *Type* drop-down list select the uplink type you want to use:

- **Failover:** In addition to the primary uplink interface one or more backup Internet uplinks operate in standby mode. All traffic is sent over the first active interface. In case of failure the uplink interface is automatically switched over to the next available interface.
- **Multipath:** All interfaces operate in active mode, and traffic is balanced automatically over all available interfaces. In case of failure the corresponding interface is excluded. Balancing is based on source IP address with a persistence time of one hour. If the interval between two requests from the same source IP address exceeds this interval the balancing is redecided. The traffic distribution is based on a simple round-robin algorithm.

3. Add interfaces to use.

Add or select at least two interfaces that should be used for uplink balancing.

Note – The sequence of the interfaces is important, especially for failover: In case of an unresponsive server the first interface following this interface is selected. You can change the interface sequence by clicking the blue arrows in the *Interfaces* box.

4. Monitoring (optional):

By default *Automatic Monitoring* is enabled to detect possible interface failures. This means that the health of all uplink balancing interfaces is monitored by having them ping a random host on the Internet at an interval of 15 seconds. If a host does not ping anymore the respective interface is regarded as dead and not used anymore for distribution.

You can define the hosts to ping by the server pool yourself:

1. Deselect the *Automatic Monitoring* checkbox.

The *Monitoring Hosts* box becomes editable.

2. Add hosts to ping.

Select or add one or more hosts that you want to ping instead of random hosts.

5. Click **Apply**.

Your settings will be saved.

A new virtual network interface named *Uplink Interfaces* is automatically created and now available for use by other functions of the Astaro Security Gateway, e.g. IPSec rules. The virtual network interface *Uplink Interfaces* comprises all uplink interfaces added to the interface list.

Additionally, a new network group named *Uplink Primary Addresses* is automatically created and now available for use by other functions of the Astaro Security Gateway, e.g. packet filter rules. It refers to the primary addresses of all *Uplink Interfaces*.

In case of an interface failure, open VPN tunnels can be automatically re-established over the next available interface provided DynDNS is used or the remote server accepts the IP addresses of all uplink interfaces. As a prerequisite, the IPSec rule must use the *Uplink Interfaces* as *Local Interface*.

Multipath Rules

On the *Network >> Interfaces >> Multipath Rules* tab you can set rules for multipath if you use the multipath mode for uplink balancing. Generally, all services are balanced without the need of creating multipath rules. Only, multipath rules allow you to additionally define the balancing of specific traffic.

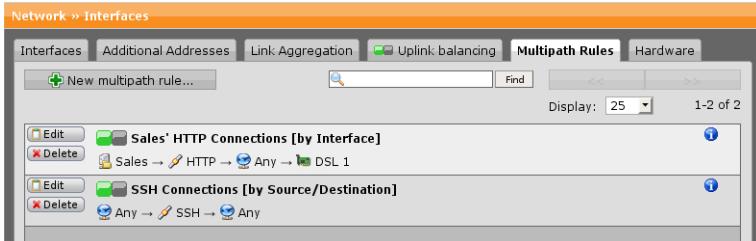


Figure 7.3 Multipath Rules

To create a multipath rule, proceed as follows:

1. **On the *Multipath Rules* tab, click *New Multipath Rule*.**

The *Create New Multipath Rule* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for the multipath rule.

Source: Select or add a source IP address or network to match.

Service: Select or add the network service to match.

Destination: Select or add a destination IP address or network that should be used for routing.

If. Persistence: *Interface persistence* is a technique which ensures that subsequent connections from a client are always routed over the same up-link interface. Persistence has a default timeout of one hour. You can decide what should be the basis for persistence:

- **By Connection:** Each connection is balanced independently.
- **By Source (Default):** Balancing is based on the source IP address.
- **By Destination:** Balancing is based on the destination IP address.
- **By Source/Destination:** Balancing is based on the source/destination IP address combination.
- **By Interface:** Select an interface from the *Bind Interface* drop-down list. All traffic applying to the rule will be routed over this interface. In

case of an interface failure and no other matching rules the connection falls back to default behavior.

Comment (optional): Add a description or other information about the multipath rule.

3. Click **Save**.

The new multipath rule is added to the *Multipath Rules* list. To either edit or delete the rule, click the corresponding buttons.

4. Enable the rule.

The new multipath rule is disabled by default. Click the status icon to activate the rule.

The rule is now enabled (status icon is green).

Hardware

The *Network >> Interfaces >> Hardware* tab lists all configured interfaces showing information such as the Ethernet mode of operation or the MAC address. For each interface, autonegotiation can be enabled or disabled.

Autonegotiation: Usually, the Ethernet mode of operation (10baseT full duplex, 10baseT half duplex, and so on) between two network devices is automatically negotiated by choosing the best possible mode of operation that are shared by the two devices, where higher speed (100 Mbit/sec) is preferred over lower speed (10 Mbit/sec), and full duplex is preferred over half duplex at the same speed.

Autonegotiation is enabled by default for network interface cards whose driver does not support the manual selection of the Ethernet operation mode or for which the respective setting could not be determined.

To change the autonegotiation setting click the *Edit* button of the respective interface card and change the setting in the appearing dialog window *Edit NIC Parameters*.

Caution – Be careful when disabling autonegotiation, as this might lead to mismatches, resulting in a significant performance decrease or even disconnect. If the respective network interface card is your interface to WebAdmin you may lose access to WebAdmin!

Bridging

Bridging is a packet forwarding technique primarily used in Ethernet networks. Unlike routing, bridging makes no assumptions about where in a network a particular address is located. Instead, it depends on broadcasting to locate unknown devices.

Through bridging, several Ethernet networks or segments can be connected to each other. The data packets are forwarded through bridging tables, which assign the MAC addresses to a bridge port. The resulting bridge will transparently pass traffic across the bridge interfaces.

Note – Such traffic must explicitly be allowed by means of appropriate packet filter rules.

Status

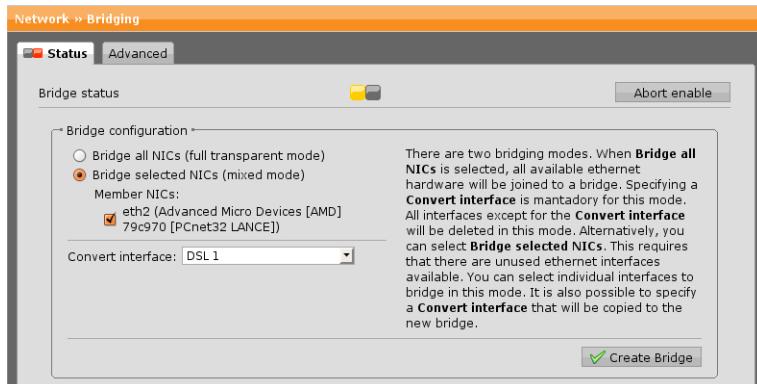


Figure 7.4 Configuring a Bridge

To configure a bridge, proceed as follows:

1. Enable bridging.

On the *Network >> Bridging >> Status* tab, either click the status icon or the *Enable* button.

The status icon turns amber and the *Bridge Configuration* area becomes editable.

2. Select the bridging mode.

You can select between two bridging modes.

- **Bridge all NICs:** If you select *Bridge all NICs*, all available Ethernet network interface cards will be joined to a bridge. Specifying a *Convert Interface* is mandatory for this mode. All interfaces except for the converted interface will be deleted in this mode.
- **Bridge Selected NICs:** You can select individual NICs that should form the bridge. This requires that there are unused network interface cards available. Select one or more of them to form the bridge. It is also possible to specify a *Convert Interface* that will be copied to the new bridge.

3. Select the interface that should be converted to a bridge.

Only an already configured interface can be selected. The bridge will inherit the address settings of that interface, as well as alias addresses and VLAN settings.

4. Click *Create Bridge*.

The network interface are being combined and the bridge is being activated (status icon shows green).

To cancel the configuration, click *Abort Enable* or the amber colored status icon.

Once the bridge has been configured, the converted interface appears as a bridge device with SysID br0 on the *Network >> Interfaces* tab. All interfaces that are members of the bridge are displayed in the *Bridge Configuration* area. To remove an interface from the bridge, clear its checkbox and click *Update Bridge*.

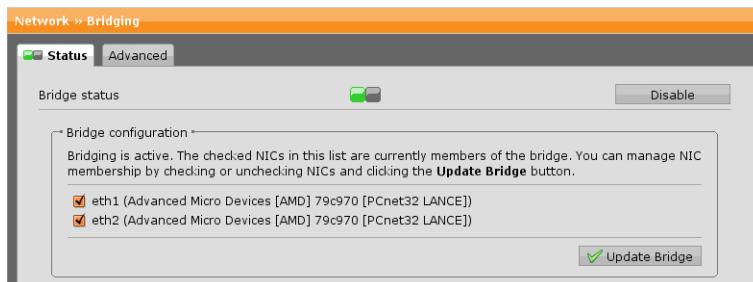


Figure 7.5 Bridging Enabled

To remove the bridge, proceed as follows:

1. On the **Status** tab, click **Disable**.

The status icon turns amber.

2. Click **Confirm Removal of Bridge**.

The status icon turns red. The bridge has been successfully removed.

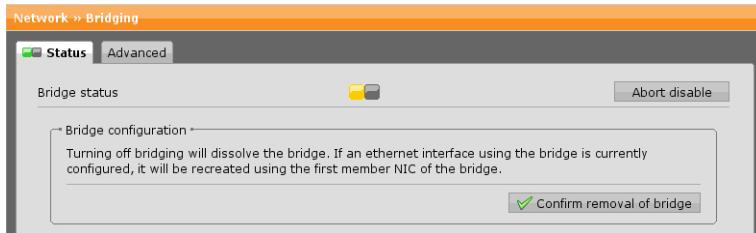


Figure 7.6 Disabling Bridging

Advanced

On the *Network >> Bridging >> Advanced* tab, the following bridging options can be configured:

Allow ARP broadcasts: The option *Allow ARP Broadcasts* lets you configure whether global ARP broadcasts should be forwarded by the bridge. If enabled, the bridge will allow broadcasts to the MAC destination address FF:FF:FF:FF:FF:FF. This, however, could be used by an alleged attacker to gather various information about the network cards employed within the respective network segment or even the security product itself. Therefore, the default setting is not to let such broadcasts pass the bridge.

Ageing Timeout: The amount of time in seconds after which an inactive MAC address will be deleted. The default time is 300 seconds.

Allow IPv6 Pass Through: Enabling this option will allow IPv6 traffic to pass the bridge without any inspection.

Static Routing

Every computer connected to a network uses a routing table to determine the path along which an outbound data packet must be sent to reach its destination. For example, the routing table contains the information whether the destination address is on the local network or if the data packet must be forwarded to a router. If a router is involved, the table contains information about which router is to be used for which network.

Two types of routes can be added to the routing table of Astaro Security Gateway: standard static routes and policy routes. With static routes, the routing target is exclusively determined by the packet's destination address. With policy routes, however, it is possible to make routing decisions based on the source interface, source address, service, or destination address.

Note – You do not need to set additional routes for networks attached to the firewall's interfaces, as well as default routes. The system inserts these routes automatically.

Standard Static Routes

The system automatically inserts routing entries into the routing table for networks that are directly connected to the system. Manual entries are necessary in those cases where there is an additional router which is to be accessed via a specific network. Routes for networks, that are not directly connected and that are inserted to the routing table via a command or a configuration file, are called static routes.

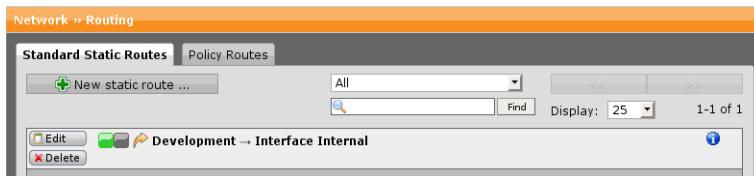


Figure 7.7 Static Routes Table

To add a standard static route, proceed as follows:

1. Click New Static Route.

The *Create New Static Route* dialog box opens.

2. Make the following settings:

Route Type: The following route types are available:

- **Interface route:** Packets are sent out on a particular interface. This is useful in two cases. First, for routing on dynamic interfaces (PPP), because in this case the IP address of the gateway is unknown. Second, for defining a default route having a gateway located outside the directly connected networks.
- **Gateway Route:** Packets are sent to a particular host (gateway).
- **Blackhole Route:** Packets are discarded silently, that is, no ICMP messages are sent to the sender. This is useful in connection with OSPF or other dynamic adaptive routing protocols to avoid routing loops, route flapping, and the like.

Network: Select the destination networks of data packets the firewall must intercept.

Interface: Select the interface through which the data packets will leave the firewall (only available if you selected *Interface Route* as route type).

Gateway: Select the gateway/router to which the firewall will forward data packets (only available if you selected *Gateway Route* as route type).

Comment (optional): Add a description or other information about the route.

3. Click Save.

The new route appears on the *Standard Static Route* list.

4. Enable the route.

Click the status icon to activate the route.

To either edit or delete a route, click the corresponding buttons.

Policy Routes

When a router receives a data packet, it normally decides where to forward it based on the destination address in the packet, which is then used to look up an entry in a routing table. However, in some cases, there may be a need to forward the packet based on other criteria. Policy-based routing allows for forwarding or routing of data packets according to your own policies.

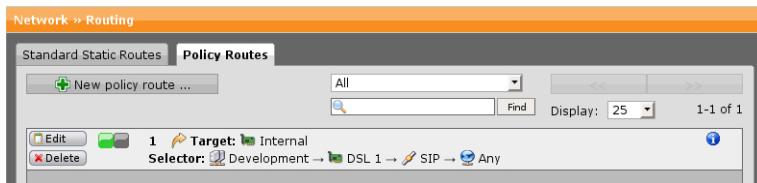


Figure 7.8 Policy Routes Table

To add a policy route, proceed as follows:

1. **Click New Policy Route.**

The *Create New Policy Route* dialog box opens.

2. **Make the following settings:**

Position: The position number, defining the priority of the policy route. Lower numbers have higher priority. Routes are matched in ascending order. Once a route has matched, routes with a higher number will not be evaluated anymore.

Route Type: The following route types are available:

- **Interface route:** Packets are sent out on a particular interface. This is useful in two cases. First, for routing on dynamic interfaces (PPP), because in this case the IP address of the gateway is unknown. Second, for defining a default route having a gateway located outside the directly connected networks.
- **Gateway Route:** Packets are sent to a particular host (gateway).

Source Interface: The interface on which the data packet to be routed has arrived. The *Any* setting applies to all interfaces.

Source Network: The source network of the data packets to be routed. The *Any* setting applies to all networks.

Service: The service definition that matches the data packet to be routed. The drop-down list contains all predefined services as well as the services you have defined yourself. These services allow you to specify precisely which kind of traffic should be processed. The *Any* setting matches any combination of protocols and source and destination ports.

Destination Network: The destination network of the data packets to be routed. The *Any* setting applies to all networks.

Target Interface: The interface for the data packets to be sent to (only available if you selected *Interface Route* as route type).

Gateway: Select the gateway/router to which the firewall will forward data packets (only available if you selected *Gateway Route* as route type).

Comment (optional): Add a description or other information about the route.

3. Click *Save*.

The new route appears on the *Policy Routes* list.

4. Enable the route.

Click the status icon to activate the route.

To either edit or delete a route, click the corresponding buttons.

Dynamic Routing (OSPF)

The *Open Shortest Path First* (OSPF) protocol is a link-state hierarchical routing protocol primarily used within larger autonomous system networks. Astaro Security Gateway supports OSPF version 2. Compared to other routing protocols, OSPF uses cost as its routing metric. The cost of an OSPF-enabled interface is an indication of the overhead required to send packets across a certain interface. The cost of an interface is inversely proportional to the bandwidth of that interface. Therefore, a higher bandwidth indicates a lower cost. For example, there is more overhead (higher cost) and time delays involved in crossing a 56 Kbit/s serial line than crossing a 10 Mbit/s Ethernet line.

The OSPF specification does not specify how the cost of an attached network should be computed—this is left to the vendor. Therefore you are free to define your own computation formula. However, if your OSPF network is adjacent to other networks that have cost already defined, you are advised to apply the same computation base.

By default, the cost of an interface is calculated based on the bandwidth. Cisco, for example, computes the cost by dividing 10^8 through the bandwidth of the interface in bits per second. Using this formula, it will cost $10^8/10000000 = 10$ to cross a 10 Mbit/s Ethernet line, whereas it will cost $10^8/1544000 = 64$ to cross a 1.544 Mbit/s line (T1) (note that the cost is rounded down to the nearest integer).

Global

On the *Network >> Dynamic Routing (OSPF) >> Global* tab you can make the basic settings for OSPF. Before you can enable the OSPF function, you must have at least one OSPF area configured (on the *Network >> Dynamic Routing (OSPF) >> Area* tab).

Caution – Configuring the OSPF function of Astaro Security Gateway requires a technically adept and experienced administrator who is familiar with the OSPF protocol. The descriptions of configuration options given here are by far not sufficient to provide a comprehensive understanding of the OSPF protocol. You are thus advised to use this feature with caution, as a misconfiguration may render your network inoperable.

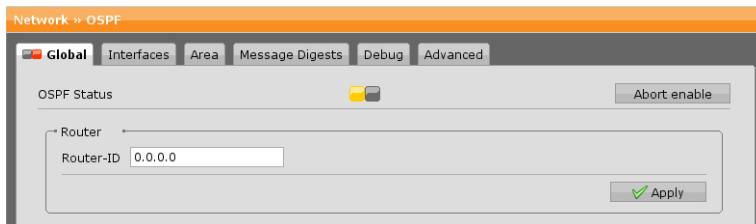


Figure 7.9 Enabling OSPF

To configure OSPF, proceed as follows:

1. **On the Area tab, create at least one OSPF area.**
2. **On the Global tab, enable OSPF.**
You can either click the status icon or the *Enable* button.
The status icon turns amber and the Router area becomes editable.
3. **Enter the router ID.**
Enter a unique router ID to identify the Astaro Security Gateway device to other OSPF routers.
4. **Click *Apply*.**
Your settings will be saved.

To disable OSPF click the status icon or *Disable*.

Interfaces

On the *Network >> Dynamic Routing (OSPF) >> Interfaces* tab you can create interface definitions to be used within an OSPF area. Each definition contains various parameters that are specific for OSPF-enabled interfaces.

To create an OSPF interface definition, proceed as follows:

1. On the **Interfaces tab**, click **New OSPF Interface**.

The *Create New OSPF Interface* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for this interface.

Interface: Select the interface to associate with this OSPF interface definition.

Auth-Type: Select the authentication type used for all OSPF packets sent and received through this interface. The following authentication types are available:

- **MD5:** Select to enable MD5 authentication. MD5 (Message-Digest algorithm 5) is a widely-used cryptographic hash function with a 128-bit hash value.
- **Plain-Text:** Select to enable plain-text authentication. The password is transmitted in clear text over the network.
- **Off:** Select to disable authentication.

Message Digest: Select the message digest (MD) to specify that MD5 authentication is used for this OSPF interface. Note that to select a message digest here it must have been created on the *Network >> Dynamic Routing (OSPF) >> Message Digests* tab first.

Cost: The cost of sending a data packet on this interface. Valid values for cost are in the range from 1 to 65535.

Advanced Options (optional): Selecting the *Advanced Options* checkbox will reveal further configuration options:

- **Hello Interval:** Specify the period of time (in seconds) that Astaro Security Gateway waits between sending *Hello* packets through this interface. The default value is ten seconds.
- **Retransmit Interval:** Specify the period of time (in seconds) between link state advertisement (LSA) retransmissions for the interface when an acknowledgment for the LSA is not received. The default value is five seconds.
- **Dead Interval:** Specify the period of time (in seconds) Astaro Security Gateway waits to receive a *Hello* data packet through the interface. The default value is 40 seconds. By convention, the *Dead Interval* value is four times greater than the value for the *Hello Interval*.

- **Priority:** Specify the router priority, which is an 8-bit number ranging from 1 to 255 primarily used in determining the designated router (DR) for the particular network. The default value is 1.
- **Transmit Delay:** Specify the estimated period of time (in seconds) it takes to transmit a link state update packet on the interface. The range is from 1 to 65535 seconds; the default value is 1.

Comment (optional): Add a description or other information about the interface.

3. Click Save.

The OSPF interface definition appears on the *Interfaces* tab.

To either edit or delete an OSPF interface, click the corresponding buttons.

Open Live Log: The OSPF Live Log log all activities on the OSPF interface. Click the button to open the live log in a new window.

Area

An OSPF network is divided into areas. These are logical groupings of routers whose information may be summarized towards the rest of the network. Areas are identified by a 32-bit ID in dot-decimal notation similar to the notation of IP addresses.

Altogether, there are six types of OSPF areas:

- **Backbone:** The area with ID 0 (or 0.0.0.0) is reserved for the OSPF network backbone, which forms the core of an OSPF network—all other areas are connected to it.
- **Normal:** A normal or regular area has a unique ID ranging from 1 (or 0.0.0.1) to 4,294,967,295 (or 255.255.255.255). Normal areas handle external routes by flooding them bi-directionally across the *Area Border Router* (ABR). Note that external routes are defined as routes which were distributed in OSPF from another routing protocol.
- **Stub:** Typically, a stub area does not have direct connections to any external networks. Injecting external routes into a stub area is unnecessary because all traffic to external networks must be routed through an *Area Border Router* (ABR). Therefore, a stub area substitutes a default route for external routes to send traffic to external networks.

- **Stub No-Summary:** A *Stub No-Summary* or *totally stubby area* is similar to a stub area, however this area does not allow so-called summary routes, that is, it restricts type 3 summary link state advertisements (LSAs) from flowing into the area.
- **NSSA:** A not-so-stubby area (NSSA) is a type of stub area that in contrast to stub areas can support external connections. Note that NSSAs do not support virtual links.
- **NSSA No-Summary:** A *NSSA No-Summary* is similar to a NSSA, however this area does not allow so-called summary routes, that is, it restricts type 3 summary link state advertisements (LSAs) from flowing into the area.

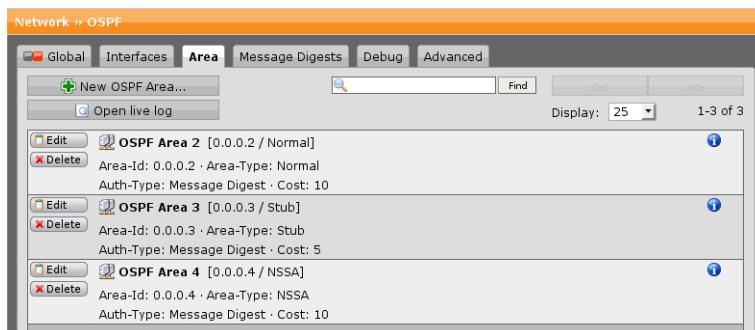


Figure 7.10 OSPF Area List

To create an OSPF area, proceed as follows:

1. **On the Area tab, click New OSPF Area.**

The *Create New OSPF Area* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for the area.

Area ID: Enter the ID of the area in dot-decimal notation (e.g., 0.0.0.1 for a normal area or 0.0.0.0 for the backbone area).

Area Type: Select an area type (see description above) to specify the characteristics of the network that will be assigned to the area in question.

Auth-Type: Select the authentication type used for all OSPF packets sent and received through the interfaces in the area. The following authentication types are available:

- **MD5:** Select to enable MD5 authentication. MD5 (Message-Digest algorithm 5) is a widely-used cryptographic hash function with a 128-bit hash value.
- **Plain-Text:** Select to enable plain-text authentication. The password is transmitted in clear text over the network.
- **Off:** Select to disable authentication.

Connect Via Interface: Select an OSPF-enabled interface. Note that to specify an OSPF-enabled interface here it must have been created on the *Network >> Dynamic Routing (OSPF) >> Interfaces* tab first.

Connect Virtual Links: All areas in an OSPF *autonomous system* (AS) must be physically connected to the backbone area (area 0). In some cases where this physical connection is not possible, you can use a virtual link to connect to the backbone through a non-backbone area. In the *Connect Virtual Links* box, enter the router ID associated with the virtual link neighbor in decimal dot notation (e.g., 10.0.0.8).

Cost: The cost of sending or receiving a data packet in this area. Valid values for cost are in the range from 1 to 65535.

Comment (optional): Add a description or other information about the area.

3. Click Save.

The new area definition appears on the *Area* tab.

To either edit or delete an OSPF area, click the corresponding buttons.

Open Live Log: The OSPF Live Log log all activities on the OSPF interface. Click the button to open the live log in a new window.

Message Digests

On the *Network >> Dynamic Routing (OSPF) >> Message Digests* tab so-called message digest keys can be generated. Message digest keys are needed to enable MD5 authentication with OSPF. MD5 authentication uses the password to generate a message digest, which is a 128-bit checksum of the data packet and password. The message digest is sent with the data packet along with a key ID associated with the password.

Note – The receiving routers must be configured with an identical message digest key.

To create a message digest key, proceed as follows:

1. **On the *Message Digest* tab, click *New Message Digest Key*.**

The *Create New Message Digest Key* dialog box opens.

2. **Make the following settings:**

ID: Enter the key identifier for this message digest key; the range is from 1 to 255.

MD5-key: Enter the associated password, which must be a string of up to 16 alphanumeric characters.

3. **Click *Save*.**

The new key appears on the *Message Digests* list.

To either edit or delete a digest key, click the corresponding buttons.

Debug

The *Network >> Dynamic Routing (OSPF) >> Debug* tab shows detailed information about relevant OSPF parameters in a separate browser window. The following information is available:

- **Show IP OSPF Neighbor:** Used to display OSPF neighbor information on a per-interface basis.
- **Show IP OSPF Routes:** Used to display the current state of the routing table.
- **Show IP OSPF Interface:** Used to display OSPF-related interface information.
- **Show IP OSPF Database:** Used to display lists of information related to the OSPF database for a specific router.
- **Show IP OSPF Border-Routers:** Used to display the internal OSPF routing table entries to an *Area Border Router* (ABR) and *Autonomous System Boundary Router* (ASBR).

Advanced

On the *Network >> Dynamic Routing (OSPF) >> Advanced* tab further OSPF-related configuration options are located concerning the injection (redistribution) of routing information from a domain other than OSPF into the OSPF domain.

Note – Policy routes cannot be redistributed.

Redistribute Connected: Select if you want to redistribute routes of directly connected networks; the default metric (cost) value is 10.

Redistribute Static: Select if you want to redistribute static routes; the default metric (cost) value is 10.

Announce Default Route: Select if you want to redistribute a default route into the OSPF domain.

Note – A default route will be advertised into the OSPF domain regardless of whether it has a route to 0.0.0.0/0.

Quality of Service (QoS)

Generally speaking, *Quality of Service (QoS)* refers to control mechanisms to provide better service to selected network traffic, and to provide priority in terms of guaranteed bandwidths in particular. In Astaro Security Gateway, priority traffic is configured on the *Network >> Quality of Service (QoS)* tabs, where you can reserve guaranteed bandwidths for certain types of outbound network traffic passing between two points in the network, whereas shaping of inbound traffic is optimized internally by various techniques such as *Stochastic Fairness Queueing* (SFQ) or *Random Early Detection* (RED).

Status

The *Status* tab lists the interfaces for which QoS can be configured. By default, QoS is disabled for each interface.

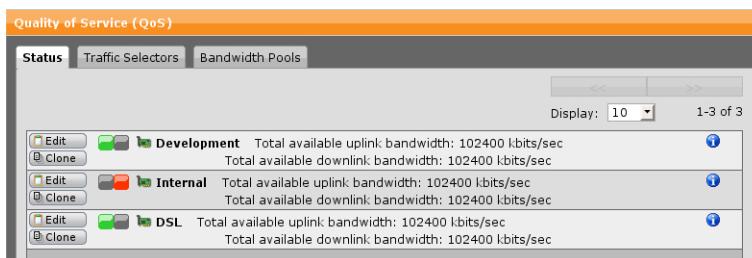


Figure 7.11 Quality of Service Status Tab

For each interface click *Edit* to configure the uplink and downlink bandwidth (in Kbit/s) provided by your ISP. For example, for a 5 Mbit/s Internet connection for both uplink and downlink, enter 5120.

If you have a fluctuating bandwidth, enter the lowest value that is guaranteed by your ISP. For example, if you have a 5 Mbit/s Internet connection for both uplink and downlink with a variation of 0.8 Mbit/s, enter 4300 Kbit/s. Note that if the available bandwidth becomes temporarily higher than the configured lowest guaranteed value, the firewall can make a projection taking the new bandwidth into account, so that the percentage bandwidth for the priority traffic will be increased as well; unfortunately, this does not work vice versa.

Limit Uplink: Selecting this option tells the QoS function to use the configured downlink and uplink bandwidth as the calculation base for prioritizing traffic that passes this interface. The *Limit Uplink* option is selected by default and should be used for the following interface types:

- Standard Ethernet interface (with a router sitting in between the firewall and the Internet—the bandwidth provided by the router is known)
- Ethernet VLAN interface (with a router sitting in between the firewall and the Internet—the bandwidth provided by the router is known)
- DSL (PPPoE)
- DSL (PPPoA)
- Modem (PPP)

Clear the *Limit Uplink* checkbox for these interfaces whose traffic shaping calculation base can be determined by the maximum speed of the interface. However, this only applies to the following interface types:

- Standard Ethernet interface (directly connected to the Internet)
- Ethernet VLAN interface (directly connected to the Internet)
- Cable Modem (DHCP)

For interfaces with no specific uplink limit given, the QoS function shapes the entire traffic proportionally. For example, if you have configured 512 Kbit/s for VoIP traffic on a Cable Modem interface and the available bandwidth has decreased by half, then 256 Kbit/s would be used for this traffic (note that proportional shaping works in both directions in contrast to interfaces that rely on a fix maximum limit).

Download Equalizer: If enabled, *Stochastic Fairness Queueing* (SFQ) and *Random Early Detection* (RED) queuing algorithms will avoid network congestion. In case the configured downlink speed is reached, packets from the most downlink consuming stream will be dropped.

Upload Optimizer: If enabled, this option will automatically prioritize outgoing TCP connection establishments (TCP packets with SYN flag set), acknowledgment packets of TCP connections (TCP packets with ACK flag set and a packet length between 40 and 60 bytes) and DNS lookups (UDP packets on port 53).

Traffic Selectors

A traffic selector can be regarded as a QoS definition which describes certain types of network traffic to be handled by QoS. These definitions later get used inside the bandwidth pool definition. There you can define how this traffic gets handled by QoS, like limiting the overall bandwidth or guarantee a certain amount of minimum bandwidth.

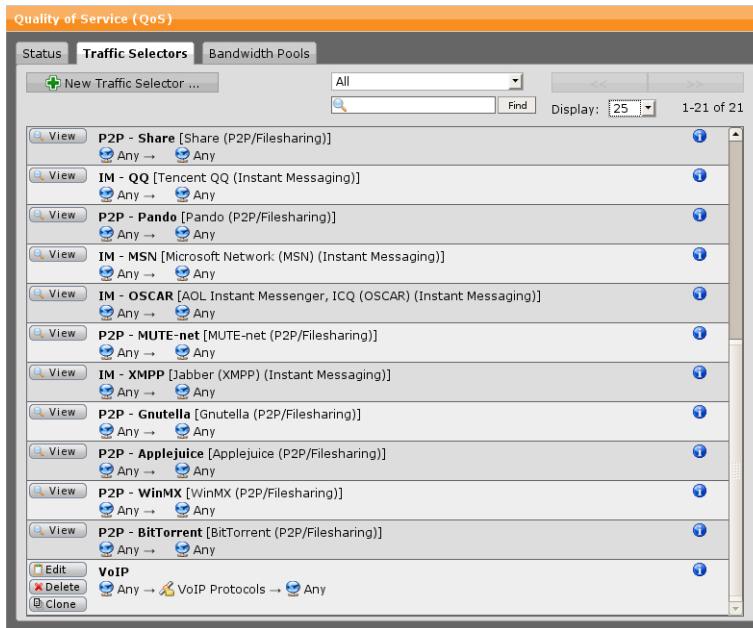


Figure 7.12 Quality of Service Traffic Selectors

To create a traffic selector, proceed as follows:

1. On the **Traffic Selector** tab, click **New Traffic Selector**.

The *Create New Traffic Selector* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for this traffic selector.

Selector Type: You can define a single traffic selector or a traffic selector group. To define a group, there must be some already defined single traffic selectors.

Source: Select the source network for which you want to enable QoS.

Service: Select the network service for which you want to enable QoS. You can select among various predefined services and service groups. For example, select VoIP protocols (SIP and H.323) if you want to reserve a fixed bandwidth for VoIP connections.

Destination: Select the destination network for which you want to enable QoS.

TOS/DSCP: Select if you want to use the *TOS/DSCP* field in the IP header to mark priority traffic. For example, in large VoIP installations, the TOS/DSCP flag is often used to mark VoIP traffic. If you do not want to reserve a fixed bandwidth for VoIP connections based on VoIP protocols, select the TOS-bits or DSCP bits used within your VoIP environment.

- **TOS-bits:** If you select TOS-bits (Type of Service), you can choose between the following settings:

- Normal service
- Minimize monetary cost
- Maximize reliability
- Maximize throughput
- Minimize delay

- **DSCP-bits:** If you select DSCP-bits (Differentiated Services Code Point), you can either specify a single *DSCP Value* (an integer in the range from 0–63) or select a predefined value from the *DSCP Class* list (e.g., *BE default dscp (000000)*).

Comment (optional): Add a description or other information about the selector.

3. Click **Save**.

The new selector appears on the *Traffic Selectors* list.

If you defined many traffic selectors, you can combine multiple selectors inside a single traffic selector group, to make the configuration more convenient.

This traffic selector or traffic selector group can now be used in each bandwidth pool. These pools can be defined on the *Bandwidth Pools* tab.

Bandwidth Pools

On the *Network >> Quality of Service >> Bandwidth Pools* tab you can define and manage bandwidth pools for bandwidth management.

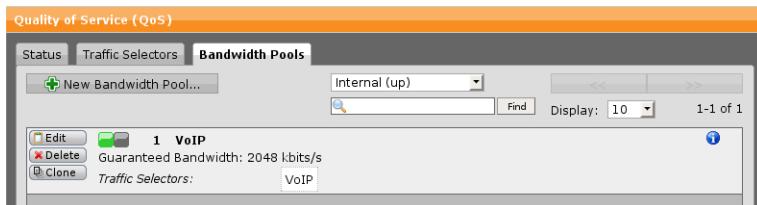


Figure 7.13 Quality of Service Bandwidth Pool

To create a bandwidth pool, proceed as follows:

1. **On the *Bandwidth Pools* tab, select an interface.**

From the drop-down list, select the interface for which you want to create a bandwidth pool.

2. **Click *New Bandwidth Pool*.**

The *Create New Bandwidth Pool* dialog box opens.

3. **Make the following settings:**

Name: Enter a descriptive name for this bandwidth pool.

Position: The position number, defining the priority of the bandwidth pool. Lower numbers have higher priority. Bandwidth pools are matched in ascending order. Once a bandwidth pool has matched, bandwidth pools with a higher number will not be evaluated anymore. Place the more specific pools at the top of the list to make sure that more vague profiles match last. For example, if you have configured a traffic selector for web traffic (HTTP) in general and for web traffic to a particular host, place the bandwidth pool that uses the latter traffic selector on top of the bandwidth pool list, that is, select position 1 for it. Note that this priority processing cannot be applied if the traffic selectors involved are assigned to different QoS-enabled interfaces.

Bandwidth: Enter the uplink bandwidth (in Kbit) you want to reserve for

this bandwidth pool. For example, if you want to reserve 1 Mbit/s for a particular type of traffic, enter 1024.

Note – You can only assign up to 90% of the entire available bandwidth to a bandwidth pool. The firewall always reserves 10% of the bandwidth for so-called unshaped traffic. To stay with the example above, if your uplink Internet connection is 5 Mbit/s and you want to assign as much bandwidth as possible to VoIP traffic, you can at most enter a value of 4608 Kbit/s.

Specify Upper Bandwidth Limit: The value you entered in the *Bandwidth* field above represents the guaranteed bandwidth to be reserved for a specific kind of traffic. However, a bandwidth pool usually allocates more bandwidth for its traffic if available. If you want a particular traffic not to consume more than a certain amount of your bandwidth, select this option to restrict the allocation of bandwidth to be used by this bandwidth pool to an upper limit.

Traffic Selector: Select the traffic selector you want to use for this bandwidth pool.

Comment (optional): Add a description or other information about this bandwidth pool.

4. Click **Save**.

The new bandwidth pool appears on the list *Bandwidth Pools*.

Multicast Routing (PIM-SM)

The menu *Network >> Multicast Routing (PIM-SM)* enables you to configure *Protocol Independent Multicast Sparse Mode* (PIM-SM) for use on your network. PIM is a protocol to dynamically route multicast packages in networks. Multicast is a technique to deliver packages that are to be received by more than one client efficiently using as little traffic as possible. Normally, packets for more than one client are simply copied and sent to every client individually, multiplying the consumed bandwidth by the number of users. Thus servers which have a lot of clients requesting the same packages at the same time, like e.g. servers for streaming content, need a lot of bandwidth.

Multicast, in contrast, saves bandwidth by sending packets only once over each link of the network. To achieve this, multicast includes adequately configured routers in the decision when to create copies on the way from the server

(sender) to the client (receiver). The routers use PIM-SM to keep track of active multicast receiver(s) and use this information to configure routing.

A rough scheme of PIM-SM communication is as follows: A sender starts transmitting its multicast data. The multicast router for the sender registers via PIM-SM with the RP router which in turn sends a join message to the sender's router. Multicast packets now flow from the sender to the RP router. A receiver registers itself via an IGMP broadcast for this multicast group at its local PIM-SM router. This router sends a join request for the receiver towards the RP router, which then in turn forwards multicast traffic to the receiver.

Multicast has its own IP address range which is 224.0.0.0/4.

Global

On the *Network >> Multicast Routing (PIM-SM) >> Global* tab you can enable and disable PIM. The *Routing Daemon Settings* area displays the status of interfaces and routers involved.

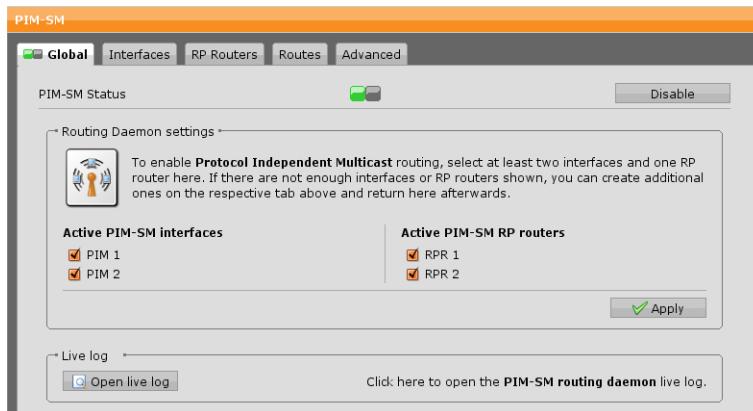


Figure 7.14 Example PIM-SM Configuration

Before you can enable PIM you need to define at least two interfaces to serve as PIM interfaces on the *Interfaces* tab and one router on the *RP Routers* tab.

To enable PIM-SM, do the following:

1. **On the *Global* tab enable PIM-SM.**

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *Routing Daemon Settings* becomes editable.

2. Make the following settings:

Active PIM-SM Interfaces: Select at least two interfaces to use for PIM-SM. Interfaces can be configured on the *Interfaces* tab.

Active PIM-SM RP Routers: Select at least one RP router to use for PIM-SM. RP routers can be defined on the *RP Routers* tab.

3. Click **Apply**.

Your settings will be saved.

PIM-SM communication is now active in your network.

To cancel the configuration, click *Abort Enable* or the amber colored status icon. To disable PIM-SM click the status icon or the *Disable* button.

Live Log

Click the *Open Live Log* button to open the PIM live log in a new window.

Interfaces

On the *Network >> Multicast Routing (PIM-SM) >> Interfaces* tab you can define over which interfaces of Astaro Security Gateway multicast communication should take place.

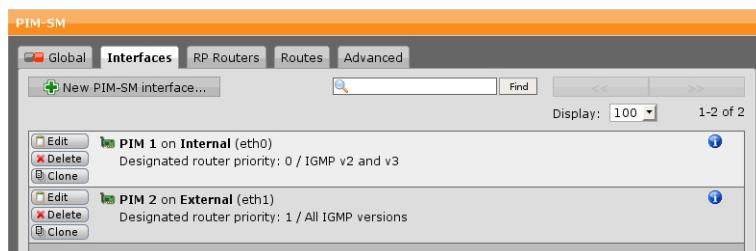


Figure 7.15 PIM-SM Interfaces List

To create a new PIM-SM interface, do the following:

1. On the *Interfaces* tab, click **New PIM-SM Interface**.

The dialog window *Create a New PIM-SM Interface* opens.

2. Make the following settings:

Name: Enter a descriptive name for PIM-SM interface.

Interface: Select an interface that is to accept PIM and IGMP network traffic.

DR priority (optional): Enter a number that defines the designated router (DR) priority for the interface. The router with the highest priority honors IGMP requests if more than one PIM-SM routers are present on the same network segment. Numbers from 0 to 2^{32} are possible. If you do not provide a priority, 0 is used by default.

IGMP: Select the version of the *Internet Group Management Protocol* that is to be supported. IGMP is used by recipients to establish multicast group memberships.

Comment (optional): Add a description or other information about the PIM-SM interface.

3. Click **Save**.

The new PIM-SM interface is added to the interfaces list.

To either edit or delete a PIM-SM interface, click the corresponding buttons.

RP Routers

In order to be able to use multicast on your network you need to configure one or more rendezvous point routers (RP routers). An RP router accepts registrations both from multicast receivers and senders. An RP router is a regular PIM-SM router that is chosen to be the RP router for certain multicast groups as well. All PIM-SM routers must agree on which router is to be the RP router.

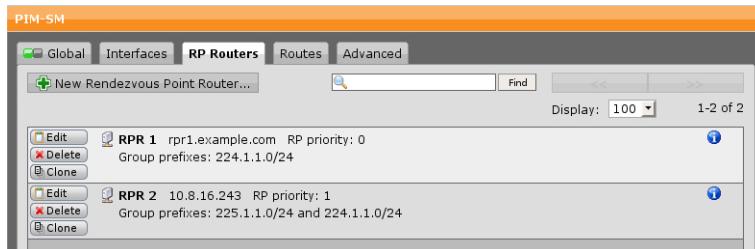


Figure 7.16 PIM-SM Rendezvous Point Routers List

To create an RP router, do the following:

1. On the **RP Routers** tab, click **New Rendezvous Point Router**.

The dialog window *Create a New RP Router* opens.

2. Make the following settings:

Name: Enter a descriptive name for the RP router.

Host: Create (or select) the host that should act as rendezvous point router.

Priority: Enter a number that defines the priority of the RP router. Join messages are sent to the RP router with the lowest priority. Numbers from 0 to 255 are possible. If you do not provide a priority, 0 is used by default.

Multicast Group Prefixes: Enter the multicast group the RP router is responsible for. You can define group prefixes like 224.1.1.0/24 if the RP is responsible for more than one multicast group. The multicast group (prefix) must be within the multicast address range which is 224.0.0.0/4.

Comment (optional): Add a description or other information about the RP router.

3. Click Save.

The new RP router is added to the routers list.

To either edit or delete an RP router, click the corresponding buttons.

Routes

You need to set up a continuous communication route between receivers and sender(s). If recipient, sender and/or RP router are not within the same network segment, you will need to create a route to enable communication between them.

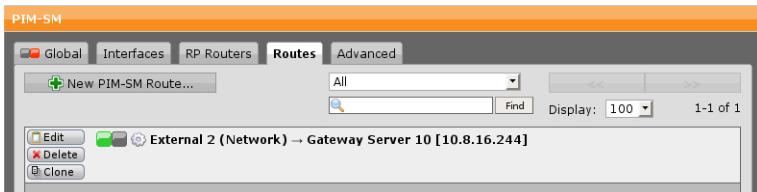


Figure 7.17 PIM-SM Routes List

To create a PIM-SM route, do the following:

1. On the **Routes** tab, click **New PIM-SM route**.

The dialog window *Create a New PIM-SM Route* opens.

2. Make the following settings:

Route Type: The following route types are available:

- **Interface route:** Packets are sent out on a particular interface. This is useful in two cases. First, for routing on dynamic interfaces (PPP), because in this case the IP address of the gateway is unknown. Second,

for defining a default route having a gateway located outside the directly connected networks.

- **Gateway Route:** Packets are sent to a particular host (gateway).

Network: Select the destination address range where the PIM traffic is to be routed to.

Gateway: Select the gateway/router to which the firewall will forward data packets (only available if you selected *Gateway Route* as route type).

Interface: Select the interface to which the firewall will forward data packets (only available if you selected *Interface Route* as route type).

Comment (optional): Add a description or other information about the route.

3. Click **Save**.

The new PIM-SM route is added to the routes list.

To either edit or delete a PIM-SM route, click the corresponding buttons.

Advanced

On the *Network >> Multicast Routing (PIM-SM) >> Advanced* tab you can configure some advanced settings for PIM.

Shortest Path Tree Settings

In some networks the PIM communication route between sender, RP, and recipient is not the shortest network path possible. The option *Enable Switch to Shortest Path Tree* allows to move an existing communication between sender and recipient to the shortest path available, omitting the RP as moderator, when a certain traffic threshold is reached.

Auto Packet Filter Settings

With this option enabled, the system will automatically create all necessary packet filter rules needed to forward multicast traffic for the specified multicast groups.

Debug Settings

Select the option *Enable Debug Mode* to see additional debugging information in the PIM-SM routing daemon log.

Uplink Monitoring

The menu *Network >> Uplink Monitoring* gives you the possibility to monitor your uplink connection and to define certain actions which will be automatically applied in case the connection status changes.

Global

On the *Network >> Uplink Monitoring >> Global* tab you can enable or disable uplink monitoring.

To enable uplink monitoring, either click the *Enable* button or the status icon. The status icon turns green. The *Uplink Status* section will either display *ON-LINE* if the uplink connection is established, or *OFFLINE* if the uplink connection is down. To cancel the configuration, click *Abort Enable* or the amber colored status icon.

Actions

On the *Network >> Uplink Monitoring >> Actions* tab you can define actions that will be automatically applied in case the uplink connection status changes. For example, you might want to disable an additional address, when your uplink connection is down.

To create a new action, do the following:

1. On the **Actions** tab, click **New Action**.

The dialog window *Create New Action If Uplink Goes Offline* opens.

2. Make the following settings:

Name: Enter a descriptive name for the action.

Type: Select the connection type for which you want to define an action.

- **IPSec Tunnel:** Select this option from the drop-down list if you want to define an action for an IPSec tunnel.
- **Additional Address:** Select this option from the drop-down list if you want to define an action for an additional address.

IPSec Tunnel: (Only available with Type *IPSec Tunnel*.) If there are any IPSec tunnels defined, you can select one of them here. For more information on IPSec tunnels see chapter *Remote Access >> IPSec*.

Add. Address: (Only available with Type *Additional Address*.) If there are any additional addresses defined, you can select one of them here. For

more information on additional addresses see chapter *Network >> Interfaces >> Additional Addresses*.

Action: You can either select *Enable* or *Disable* here, which means that, in case of an uplink interruption, the above selected IPSec tunnel or additional address is going to be enabled or disabled.

Comment (optional): Add a description or other information about the action.

3. Click **Save**.

The action will be saved and applied in case the uplink connection is interrupted.

To either edit or delete an action, click the corresponding buttons.

Advanced

On the *Network >> Uplink Monitoring >> Advanced* tab you can disable automatic monitoring of the uplink connection and define one or more hosts instead which are used for monitoring. These hosts will then be pinged in certain periods and if none of them is reachable, the uplink connection is regarded as down. Subsequently, the actions defined on the *Actions* tab will be carried out.

To use your own hosts for monitoring, do the following:

1. Unselect the checkbox **Automatic Monitoring**.

The object box *Monitoring Hosts* becomes editable.

2. Add one or more hosts to the **Monitoring Hosts** box.

You can either select the host(s) from the object list or create new hosts.

3. Click **Apply**.

Your settings will be saved.

The hosts defined will now be used for monitoring.

Network Services

This chapter describes how to configure several network services of Astaro Security Gateway for your network.

The following topics are included in this chapter:

- DNS
- DHCP
- NTP

DNS

The tabs of the *Network Services >> DNS* menu contain miscellaneous configuration options, all related to the *Domain Name System* (DNS), a system primarily used to translate domain names (computer hostnames) to IP addresses.

Global

On the *Network Services >> DNS >> Global* tab you can specify the networks that are to be allowed to use the firewall as a recursive DNS resolver. Typically, you will select your internal networks here.

Note – If you already run an internal DNS server, for example as part of Active Directory, you should leave this box empty.

Flush Resolver Cache

The DNS proxy uses a cache for its records. Each record has an expiration date (TTL, time-to-live) at which it will be deleted, which is normally one day. However, you can empty the cache manually e.g. if you want recent changes in DNS records to take effect immediately, not having to wait for the TTL to expire. To empty the cache, click *Flush Resolver Cache Now*.

Forwarders

On the *Network Services >> DNS >> Forwarders* tab you can specify so-called DNS forwarders. A DNS forwarder is a *Domain Name System* (DNS) server on a network used to forward DNS queries for external DNS names to DNS servers outside of that network. If possible, add a DNS forwarder to your configuration. This should be a host "near" your site, preferably one provided by your Internet provider. It will be used as a "parent" cache. This will speed up DNS requests considerably. If you do not specify a forwarding name server, the root DNS servers will be queried for zone information first, taking a longer time to complete requests.

To select a DNS forwarder, proceed as follows:

1. Select a DNS forwarder.

Select or add a DNS forwarder.

2. Use Forwarders Assigned by ISP (optional).

Select the *Use Forwarders Assigned by ISP* checkbox to forward DNS queries to the DNS servers of your ISP. When this box is checked, all forwarders automatically assigned by your ISP will be listed in the line below the box.

3. Click *Apply*.

Your settings will be saved.

Request Routing

Suppose you run your own internal DNS server, this server could be used as an alternate server to resolve DNS queries for a domain you do not want to be resolved by DNS forwarders. On the *Network Services >> DNS >> Request Routing* tab you can define routes to your own DNS servers.

To create DNS request routes, proceed as follows:

1. On the *Request Routing* tab, click *New DNS Request Route*.

The *Create New DNS Request Route* dialog box opens.

2. Make the following settings:

Domain: Enter the domain for which you want to use an alternate DNS server.

Target Servers: Select one or more DNS servers to use for resolving the domain entered above.

Comment (optional): Add a description or other information about the DNS request route.

3. Click Save.

The new route appears on the *DNS Request Route* list and is immediately active.

To either edit or delete a DNS request route, click the corresponding buttons.

Static Entries

If you do not want to set up your own DNS server but need a static DNS mapping for a few hosts of your network, you can enter these mappings here. Note that this only scales for a limited number of entries and is by no means intended as a replacement of a fully operable DNS server.

To create a static mapping, proceed as follows:

1. On the *Static Entries* tab, click *New Static DNS Mapping*.

The *Create New Static DNS Mapping* dialog box opens.

2. Make the following settings:

Hostname: Enter the hostname for which you want to define a static DNS mapping.

IP Address: Enter the IP address of that host.

Comment (optional): Add a description or other information about the static mapping.

3. Click Save.

The new mapping appears on the *DNS Mapping* list.

To either edit or delete a static entry, click the corresponding buttons.

DynDNS

Dynamic DNS, or DynDNS for short, is a domain name service which allows static Internet domain names to be assigned to a computer with a varying IP address. You can sign up for the DynDNS service at the DynDNS website²⁰ to get a DNS alias that will automatically be updated when your uplink IP address changes. Once you have registered to this service, you will receive a hostname, username, and password, which are necessary for the configuration.

²⁰ <http://www.dyndns.com/>

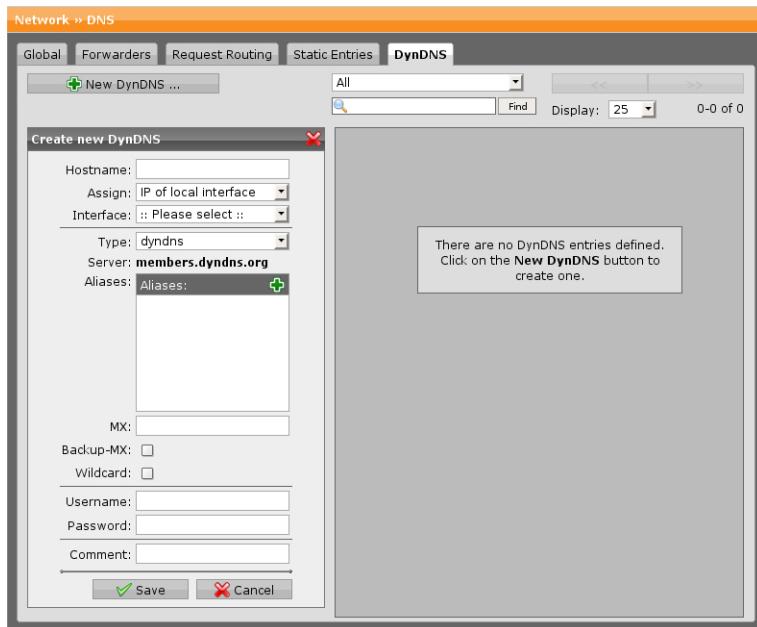


Figure 8.1 Configuring DynDNS

To configure DynDNS, proceed as follows:

1. **On the *DynDNS* tab, click *New DynDNS*.**

The *Create New DynDNS* dialog box opens.

2. **Make the following settings:**

Hostname: Enter the domain you received from your DynDNS service provider (e.g., example.dyndns.org). Note that you need not adhere to a particular syntax for the hostname to be entered here. What you must enter here exclusively depends on what your DynDNS service provider requires. Apart from that, you can also use your DynDNS hostname as the firewall's main hostname, which, however, is not mandatory.

Assign: Define the IP the DynDNS name is to be associated with. Selecting *IP of Local Interface* is useful when the interface in question has a public IP address. Typically, you will use this option for your DSL uplink. When you select *First Public IP on the Default Route* no interface needs to be specified. Instead, your ASG will send a WWW request to a public DynDNS server which in return will respond with the public IP you are currently using. This is useful when your ASG does not have a public IP address but

is located inside a private network, connected to the Internet via a masquerading router.

Interface: Select the interface for which you want to use the DynDNS service, most likely this will be your external interface connected to the Internet.

Type: The following DynDNS types are available:

- **DynDNS:** Select this option if you are using DynDNS' standard DNS service.
- **DynDNS-custom:** Select this option if you are using DynDNS' custom DNS service. Custom DNS is designed primarily to work with domains owned or registered by yourself.

Aliases (optional): Use this dialog box to enter additional hostnames which should point to the same IP address as the main hostname above (e.g., mail.example.com, example.com).

MX (optional): Mail exchangers are used for directing mail to specific servers other than the one a hostname points to (only available if you selected *DynDNS* as *DynDNS Type*). MX records serve a specific purpose: they let you specify the host (server) to which mail for a specific domain should be sent. For example, if you enter mail.example.com as Mail Exchanger, mail addressed to user@example.com would be delivered to the host mail.example.com.

Backup-MX (optional): Select this checkbox only if the hostname named in the *Hostname* text box is to serve as main mail exchanger. Then the hostname from the *MX* text box will only be advertised as a backup mail exchanger.

Wildcard (optional): Select this option if you want subdomains to point to the same IP address as your registered domain (only available if you selected *DynDNS* as *DynDNS Type*). Using this option an asterisk (*) will be added to your domain serving as a wildcard (e.g., *.example.dyndns.org), thus making sure that, for example, www.example.dyndns.org will point to the same address as example.dyndns.org.

Username: Enter the username you received from the DynDNS service provider.

Password: Enter the password you received from the DynDNS service provider.

Comment (optional): Add a description or other information about the DynDNS.

3. Click Save.

The new DynDNS appears on the DynDNS service list. The service is still disabled (status icon is red).

4. Enable DynDNS.

Click the status icon to enable the DynDNS service.

The service is now enabled (status icon is green).

To either edit or delete a DynDNS, click the corresponding buttons.

You can use multiple DynDNS objects at the same time. When all settings for two hostnames are identical, it is recommended to use the *Aliases* option—instead of creating two distinct objects.

DHCP

The *Dynamic Host Configuration Protocol* (DHCP) automatically distributes addresses from a defined IP address pool to client computers. It is designed to simplify network configuration on large networks, and to prevent address conflicts. DHCP distributes IP addresses, default gateway information, and DNS configuration information to its clients.

In addition to simplifying the configuration of client computers and allowing mobile computers to move painlessly between networks, DHCP helps to localize and troubleshoot IP address-related problems, as these are mostly issues with the configuration of the DHCP server itself. It also allows for a more effective use of address space, especially when not all computers are active at the same time, as addresses can be distributed as needed and reused when unneeded.

Servers

The tab *Network Services >> DHCP >> Server* allows to configure a DHCP server. The security system provides the DHCP service for the connected network. The DHCP server can be used to assign basic network parameters to your clients. You can run the DHCP service on multiple interfaces, with each interface having its own configuration set.

To configure a DHCP server, proceed as follows:

1. On the Server tab, click New DHCP Server.

The *Create New DHCP Server* dialog box opens.

2. Make the following settings:

Interface: The interface from which the IP addresses should be assigned to

the clients. You can only select an already configured interface.

Range Start/End: The IP range to be used as an address pool on that interface. By default, the configured address area of the network card will appear in the text boxes. The range must be inside the network attached to the interface.

DNS Server 1/2: The IP addresses of the DNS servers.

Default Gateway: The IP address of the default gateway.

Domain (optional): Enter the domain name that will be transmitted to the clients (e.g., `intranet.example.com`).

Lease Time: Each IP address assigned by the DHCP server expires after a certain interval. Here you can define this interval in seconds. The default is 86400 seconds (one day). The minimum is 600 seconds (10 minutes) and the maximum is 2592000 seconds (one month).

Clients with Static Mappings Only (optional): Select this option to have the DHCP server assign IP addresses only to clients that have an entry on the *Static MAC/IP Mappings* tab.

WINS Node Type: *Windows Internet Naming Service* (WINS) is Microsoft's implementation of *NetBIOS Name Server* (NBNS) on Windows, a name server and service for NetBIOS computer names. A WINS server acts as a database that matches computer names with IP addresses, thus allowing computers using NetBIOS to take advantage of the TCP/IP network. The following WINS node types are available:

- **Do not set:** The WINS node type is not set and will be chosen by the client.
- **B-node (no WINS):** B-node systems use broadcasts only.
- **P-node (WINS only):** P-node systems use only point-to-point name queries to a Windows name server (WINS).
- **M-node (Broadcast, then WINS):** M-node systems broadcast first, then query the name server.
- **H-node (WINS, then Broadcast):** H-node systems query the name server first, then broadcast.

WINS Server: Depending on your WINS node type selection, this text box appears. Enter the IP address of the WINS server.

Enable HTTP Proxy Auto Configuration: Select this option if you want to provide a PAC file for automatic proxy configuration of browsers. For more information see chapter *Web Security >> HTTP/S >> Advanced*, section *Proxy Auto Configuration*.

Comment (optional): Add a description or other information about the DHCP server.

3. Click *Save*.

The new DHCP server definition appears on the DHCP server list and is immediately active.

To either edit or delete a DHCP server definition, click the corresponding buttons.

Relay

The *Network Services >> DHCP >> Relay* tab allows you to configure a DHCP relay. The DHCP service is provided by a separate DHCP server and the security system works as a relay. The DHCP relay can be used to forward DHCP requests and responses across network segments. You need to specify the DHCP server and a list of interfaces between which DHCP traffic shall be forwarded.

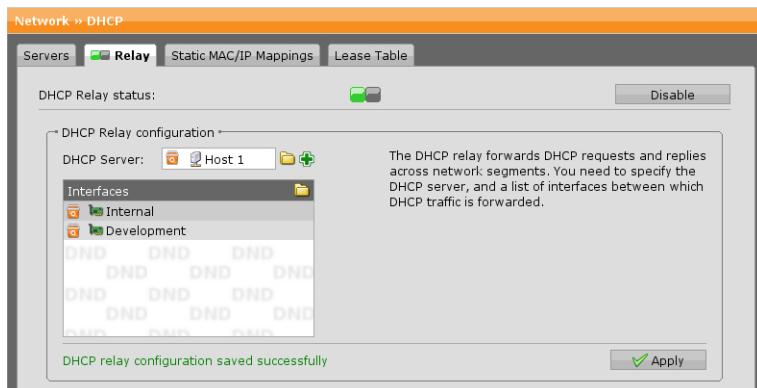


Figure 8.2 Configuring a DHCP Relay

To configure a DHCP relay, proceed as follows:

1. On the *Relay* tab, enable *DHCP Relay*.

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *DHCP Relay Configuration* area becomes editable.

2. Select the *DHCP server*.

3. Select an interface.

DHCP requests arriving on these interfaces will be forwarded to the selected DHCP server.

4. Click *Apply*.

Your settings will be saved.

To cancel the configuration, click *Abort Enable* or the amber colored status icon.

Static MAC/IP Mappings

On the *Network Services >> DHCP >> Static MAC/IP Mappings* tab you can assign static MAC address to IP addresses mappings for some or all clients. For that purpose, you need a configured DHCP server and the MAC address of the client's network card. The MAC addresses are usually specified in a format consisting of six groups of two hexadecimal digits, separated by colons (e.g., 00:04:76:16:EA:62).

Note – To avoid an IP address clash between regularly assigned addresses from the DHCP pool and those statically mapped make sure that the latter are not in the scope of the DHCP pool. For example, a static mapping of 192.168.0.200 could result in two systems receiving the same IP address if the DHCP pool is 192.168.0.100-192.168.0.210.

To create a static MAC/IP address mapping, proceed as follows:

1. On the *Static MAC/IP Mappings* tab, click *New MAC/IP Mapping*.

The *Create New MAC/IP Mapping* dialog box opens.

2. Make the following settings:

DHCP Server: The DHCP server to be used for static MAC/IP mappings.

MAC Address: The MAC address of the client's network interface card.

IP Address: The IP address of the client. The IP address must be within the address range of the network interface card.

Comment (optional): Add a description or other information about the MAC/IP mapping.

3. Click *Save*.

The new mapping appears on the static MAC/IP mapping list.

To either edit or delete a static MAC/IP mapping, click the corresponding buttons.

Lease Table

Using DHCP, a client no longer owns an IP address, but rather *leases* it from the DHCP server, which gives permission for a client to use the address for a period of time.

Hostname	MAC address	IP address	Lease start	Lease expiry	Add static mapping
[Unknown]	00:10:f3:0b:cb:e3	10.8.3.43	2009/06/30 09:34:16 UTC	2009/07/01 09:34:16 UTC	New mapping
talex	00:48:54:86:4e:cc	10.8.3.254	2009/06/30 09:35:24 UTC	2009/07/01 09:35:24 UTC	New mapping
talex	00:04:23:9f:1f:16	10.8.2.255	2009/06/30 09:35:27 UTC	2009/07/01 09:35:27 UTC	New mapping

Figure 8.3 DHCP Lease Table

The *Lease Table* on the *Network Services >> DHCP >> Lease Table* tab shows the current leases issued by the DHCP server, including information about the start date and the date when the lease will expire.

Add Static Mapping

You can use an existing lease as template for a new static MAC/IP mapping, by using the *New Mapping* button in the *Add Static Mapping* column of the table. Do the following:

1. Click the button *New Mapping*.

The dialog window *Add Mapping* opens.

2. Make the following settings:

MAC Address (optional): Change the MAC address only if you want to assign the static mapping to a host different from your selection.

IP Address: Change the IP address to an address outside the DHCP pool range.

Create DNS Mapping (optional): Select the checkbox to automatically create a static DNS mapping for the host (see *Network Services >> DNS >> Static Entries*). If you provide a *Hostname*, this mapping will use it.

Create Network Host Object (optional): Select the checkbox to automatically create a host object (see *Definitions >> Networks*). If you provide a *Hostname*, this will be the object's name.

Hostname (optional): For convenience, it is recommended that you

provide a name for the host. Otherwise the objects will be listed as "[unknown]".

3. Click **Save**.

Your settings will be saved.

Note – When converting a lease to a static mapping you should change the IP address so that it is no longer inside the scope of the DHCP pool. However, if you change the IP address, the address used by the client will not change immediately, but only when it tries to renew its lease for the next time.

NTP

The menu *Network Services >> NTP* allows you to configure an NTP server for the connected networks. The *Network Time Protocol* (NTP) is a protocol used for synchronizing the clocks of computer systems over IP networks. Instead of just synchronizing the time of Astaro Security Gateway, which can be configured on the *Management >> System Settings >> Time and Date* tab, you can explicitly allow certain networks to use this service as well.

To enable the use of NTP time synchronization for specific network, proceed as follows:

1. Enable the NTP server.

You can either click the status icon or the *Enable* button.

2. Select **Allowed Networks**.

Select the networks that should be allowed to access the NTP server.

3. Click **Apply**.

Your settings will be saved.

Network Security

This chapter describes how to configure basic network security features of Astaro Security Gateway. The *Network Security Statistics* page in WebAdmin shows an overview of Intrusion Prevention events and dropped data packets for both source and destination hosts. Each of the sections contains a *Details* link. Clicking the link redirects you to the respective *Reporting* section of WebAdmin, where you can find more statistical information.

The following topics are included in this chapter:

- Packet filter
- Network Address Translation (NAT)
- Intrusion Prevention
- Server Load Balancing
- Advanced Settings

Packet Filter

The menu *Network Security >> Packet Filter* allows you to define and manage packet filter rules of the firewall. Generally speaking, the packet filter is the central part of the firewall which functions in a networked environment to prevent some communications forbidden by the security policy. The default security policy of Astaro Security Gateway states that all network traffic is to be blocked and logged, except for automatically generated rulesets that are necessary for other software components of the firewall to work. However, those auto-generated rulesets are not shown on the *Packet Filter >> Rules* tab. This policy requires you to define explicitly which data traffic is allowed to pass the firewall.

Rules

On the *Network Security >> Packet Filter >> Rules* you can manage the packet filter ruleset. All newly defined packet filter rules are disabled by default

once added to the rules table. Activated packet filter rules are applied in the given order until the first rule matches. The processing order is determined by the position number, so if you change the order of the rules by their position numbers, the processing order will change as well.

Caution – Once a packet filter rule matched, all other rules will be ignored. For that reason, the sequence of rules is very important. Never place a rule such as *Any (Source) – Any (Service) – Any (Destination) – Allow (Action)* at the top of the rule table, as this will allow each packet to traverse the firewall in both directions, ignoring all other rules that may follow.

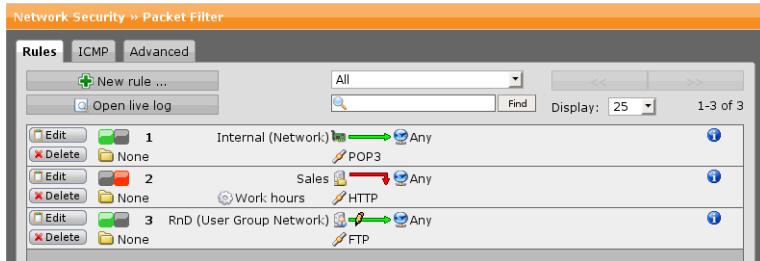


Figure 9.1 Packet Filter Rule Table

To create a packet filter rule, proceed as follows:

1. **On the Rules tab, click New Rule.**

The *Create New Rule* dialog box opens.

2. **Make the following settings:**

Group: The Group option is useful to group packet filter rules logically for better readability of the packet filter ruleset. Grouping is only used for display purposes, it does not affect rule matching.

Position: The position number, defining the priority of the rule. Lower numbers have higher priority. Rules are matched in ascending order. Once a rule has matched, rules with a higher number will not be evaluated anymore.

Source: The source network definition, describing from which host(s) or networks the packets are originating.

Service: The service definition that describes the protocol(s) and, in case of TCP or UDP, the source and destination port(s) of the packets.

Destination: The destination network definition, describing the target host(s) or network(s) of the packets.

Action: The action that describes what to do with traffic that matches the rule. The following actions can be selected:

- **Allow:** The connection is allowed and traffic is forwarded.
- **Deny:** Packets matching a rule with this action will be silently dropped.
- **Reject:** Connection requests matching rules with this action will be actively rejected. The sender will be informed via an ICMP message.

Time Event: By default, no time event is selected, meaning that the rule is always valid. If you select a time event, the rule will only be valid at the time specified by the time event definition. For more information, see Time Events.

Log Traffic: If you select this option, logging is enabled and packets matching the rule are logged in the packet filter log.

Comment (optional): Add a description or other information about the rule.

3. Click **Save**.

The new rule appears on the rule list.

4. Enable the rule.

Click the status icon to activate the rule.

To either edit or delete a rule, click the corresponding buttons.

Open Live Log: This will open a pop-up window containing a real-time log of filtered packets, whose regularly updating display shows recent network activity. The background color indicates which action has been applied:

- Red: The package was dropped.
- Yellow: The package was rejected.
- Green: The package was allowed.
- Gray: The action could not be determined.

The live log also contains information about which packet filter rule caused a packet to be rejected. Such information is essential for rule debugging.

Using the search function, you can filter the packet filter log for specific entries. The search function even allows to negate expressions by typing a dash in front of the expression, e.g. -WebAdmin which will successively hide all lines containing this expression.

Live Log: Packet filter		Filter:	<input checked="" type="checkbox"/> 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	Packetfilter rule #1	TCP	10.8.0.8:45070 → 10.8.0.28:21
09:15:02	Packetfilter 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	10.8.0.8:44829 → 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
09:15:11	Packetfilter rule #1	TCP	10.8.0.8:45074 → 10.8.0.28:21
09:15:22	Packetfilter 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	Packetfilter rule #1	TCP	10.8.0.8:45078 → 10.8.0.28:21

Figure 9.2 Packet Filter Live Log

Selecting the *Autoscroll* checkbox will automatically scroll down the window's scrollbar to always show the most recent results.

Below are some basic hints for configuring the packet filter:

- **Dropped Broadcasts:** By default, all broadcasts are dropped, which in addition will not be logged (for more information, see Advanced). This is useful for networks with many computers utilizing NetBIOS (for example, Microsoft Windows operating systems), because broadcasts will rapidly clutter up your packet filter logfile. To define a broadcast drop rule manually, group the definitions of the broadcast addresses of all attached networks, add another "global_broadcast" definition of 255.255.255.255/255.255.255.255, then add a rule to drop all traffic to these addresses on top of your packet filter configuration. On broadcast-heavy networks, this also has the benefit of increasing the system performance.
- **Rejecting IDENT Traffic:** If you do not want to use the IDENT reverse proxy, you can actively reject traffic to port 113 (IDENT) of your internal networks. This may prevent longer timeouts on services that use IDENT, such as FTP, IRC and SMTP.

Note – If you use masquerading, IDENT requests for masqueraded networks will arrive on the masquerading interface.

- Since NAT will change the addresses of network packets, it has implications on the packet filter functionality.

- DNAT is applied *before* the packet filter. This means that the packet filter will "see" the already translated packets. You must take this into account when adding rules for DNAT related services.
- SNAT and Masquerading is applied *after* the packet filter. This means that the packet filter still "sees" the untranslated packets with the original source addresses.

The control panels in the table header can be used to filter packet filter rules for specific criteria to rearrange rules for better readability. If you have defined groups you can select a group from the drop-down menu and thus see all rules that belong to this group. Using the search field you can look for a keyword or just a string to see the rules related to it. The search comprises a rule's source, destination, service, group name, and comment.

ICMP

On the *Network Security >> Packet Filter >> ICMP* tab you can configure the settings for the *Internet Control Message Protocol* (ICMP). ICMP is used to exchange connection-related status information between hosts. ICMP is important for testing network connectivity or troubleshooting network problems.

Allowing any ICMP traffic on this tab will override ICMP settings being made in the packet filter. If you only want to allow ICMP for certain hosts or networks, you should use the *Packet filter >> Rules* tab instead.

Global ICMP Settings

The following global ICMP options are available:

- **Allow ICMP on Firewall:** This option enables the firewall to respond to ICMP packets of any kind.
- **Allow ICMP through Firewall:** This option enables the forwarding of all ICMP packets through the firewall.
- **Log ICMP Redirects:** ICMP redirects are sent from one router to another to find a better route for a packet's destination. Routers then change their routing tables and forward the packet to the same destination via the supposedly better route. If you select this option, all ICMP redirects will be logged in the packet filter log.

Ping Settings

The program *ping* is a computer network tool used to test whether a particular host is reachable across an IP network. Ping works by sending ICMP echo

request packets to the target host and listening for ICMP *echo response* replies. Using interval timing and response rate, ping estimates the round-trip time and packet loss rate between hosts.

These following ping options are available:

- **Firewall Is Ping Visible:** The firewall responds to ICMP *echo request* packets. This feature is enabled by default.
- **Ping From Firewall:** You can use the ping command on the firewall. This feature is enabled by default.
- **Firewall Forwards Pings:** The firewall forwards ICMP *echo request* and *echo response* packets.

Traceroute Settings

The program traceroute is a computer network tool used to determine the route taken by packets across an IP network. It lists the IP addresses of the routers that were involved in transporting the packet. If the packet's route cannot be determined within a certain time frame, traceroute will report an asterisk (*) instead of the IP address. After a certain number of failures, the check will end. An interruption of the check can have many causes, but most likely it is caused by a packet filter along the network path that blocks traceroute packets.

The following traceroute options are available:

- **Firewall Is Traceroute Visible:** The firewall responds to traceroute packets.
- **Traceroute From Firewall:** You can use the traceroute command on the firewall. This feature is enabled by default.
- **Firewall Forwards Traceroute:** The firewall forwards traceroute packets.

Note – In addition, the UDP ports for UNIX traceroute applications are opened, too.

Advanced

The *Network Security >> Packet Filter >> Advanced* tab contains advanced settings for the packet filter and the NAT rules.

Connection Tracking Helpers

So-called connection tracking helpers enable protocols that use multiple network connections to work with packet filter or NAT rules. All connections handled by the packet filter are tracked by the `conntrack` kernel module, a process better known as *connection tracking*. Some protocols such as FTP and IRC require several ports to be opened, and hence require special connection tracking helpers supporting them to operate correctly. These helpers are special kernel modules that help identify additional connections by marking them as being related to the initial connection, usually by reading the related addresses out of the data stream.

For example, for FTP connections to work properly, the FTP `conntrack` helper must be selected. This is due to the specifics of the FTP protocol, which first establishes a single connection that is called the FTP control connection. When commands are issued through this connection, other ports are opened to carry the rest of the data (e.g., downloads or uploads) related to that specific command. The problem is that the firewall will not know about these extra ports, since they were negotiated dynamically. Therefore, the firewall will be unable to know that it should let the server connect to the client over these specific ports (active FTP connections) or to let clients on the Internet connect to the FTP server (passive FTP connections).

This is where the FTP `conntrack` helper becomes effective. This special helper is added to the connection tracking module and will scan the control connection (usually on port 21) for specific information. When it runs into the correct information, it will add that specific information to a list of expected connections as being related to the control connection. This in return enables the firewall to track both the initial FTP connection as well as all related connections properly.

Connection tracking helpers are available for the following protocols:

- FTP
- IRC (for DCC)
- PPTP
- TFTP

Note – The PPTP helper module needs to be loaded if you want to offer PPTP VPN services on the firewall. Otherwise PPTP sessions cannot be established. The reason for this is that PPTP first establishes a TCP port 1723 connection before switching to *Generic Routing Encapsulation* (GRE) communication, which

is a separate IP protocol. If the PPTP helper module is not loaded, all GRE packets will be blocked by the firewall. Alternatively, if you do not want to use the PPTP helper module, you can manually add packet filter rules allowing GRE packets for incoming and outgoing traffic.

Protocol Handling

Enable TCP Window Scaling: The TCP receive window (RWin) size is the amount of received data (in bytes) that can be buffered during a connection. The sending host can send only that amount of data before it must wait for an acknowledgment and window update from the receiving host. For more efficient use of high bandwidth networks, a larger TCP window size may be used. However, the TCP window size field controls the flow of data and is limited to 2 bytes, or a window size of 65535 bytes. Since the size field cannot be expanded, a scaling factor is used. TCP window scaling is a kernel option of the TCP/IP stack and can be used to increase the maximum window size from 65535 bytes to 1 Gigabyte. Since many network devices such as routers, load balancers, firewalls, and so on still do not fully support window scaling it will be disabled by default.

Use Strict TCP Session Handling: By default, the system can "pick up" existing TCP connections that are not currently handled in the connection tracking table due to a network facility reset. This means that interactive sessions such as SSH and Telnet will not quit when a network interface is temporarily unavailable. Once this option is enabled, a new three-way handshake will always be necessary to re-establish such sessions. It is generally recommended to leave this option turned off.

Validate Packet Length: If enabled, the packet filter will check the data packets for minimal length if the ICMP, TCP, or UDP protocol is used. If the data packets are smaller than the minimal values, they will be blocked and a record will be written to the packet filter log.

Spoof Protection: By default, spoof protection is disabled. You can choose between the following settings:

- **Normal:** The firewall will drop and log packets which either have the same source IP address as the interface itself or which arrive on an interface which has a source IP of a network assigned to another of its interfaces.
- **Strict:** The firewall will also drop and log all packets which have a destination IP for an interface but arriving on an interface other than assigned, that is, if it arrives on an interface for which it is not destined. For example, those packets will be dropped that were sent from an external network to

the IP address of the internal interface which is supposed to accept packets from the internal network only.

Logging Options

Log FTP Data Connections: The security system will log the data connections of FTP file and directory listing transfers. The log records are marked by the string "FTP data".

Log Unique DNS Requests: The security system will log all outgoing requests to DNS servers as well as their outcome. The log records are marked by the string "DNS request".

Log Dropped Broadcasts: By default, the packet filter drops all broadcasts, which in addition will not be logged. However, if you need broadcasts to be logged in the packet filter log, for example, for audit purposes, select this option.

Traffic Monitor

This section allows you to start a traffic monitor where you can follow the bandwidth consumption of all interfaces. The traffic monitor is opened in a new window, when you click the *Start Traffic Monitor* button. The traffic monitor refreshes automatically at short intervals. You can use the *Pause* button to interrupt refreshing.

Tip – The traffic monitor can also be opened for a specific interface via a click on the *In/Out* graphs on the Dashboard.

NAT

The menu *Network Security >> NAT* allows you to define and manage NAT rules of the firewall. *Network Address Translation* (NAT) is the process of rewriting the source and/or destination addresses of IP packets as they pass through a router or firewall. Most systems using NAT do so in order to enable multiple hosts on a private network to access the Internet using a single public IP address. When a client sends an IP packet to the router, NAT translates the sending address to a different, public IP address before forwarding the packet to the Internet. When a response packet is received, NAT translates the public address into the original address and forwards it to the client. Depending on system resources, NAT can handle arbitrarily large internal networks.

Masquerading

Masquerading is a special case of *Source Network Address Translation* (SNAT) and allows you to masquerade an internal network (typically, your LAN with private address space) behind a single, official IP address on a network interface (typically, your external interface connected to the Internet). SNAT is more generic as it allows to map multiple source addresses to several destination addresses.

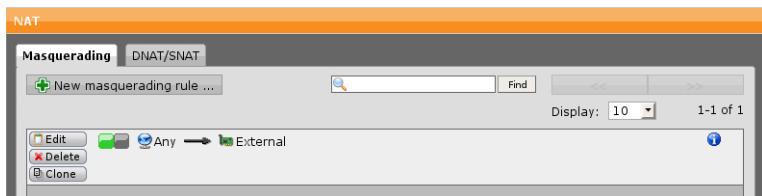


Figure 9.3 Masquerading Rule List

Note – The source address is only translated if the packet leaves the firewall system via the specified interface. Note further that the new source address is always the current IP address of that interface (meaning that this address can be dynamic).

To create a masquerading rule, proceed as follows:

1. On the **Masquerading** tab, click **New Masquerading Rule**.
The *Create New Masquerading Rule* dialog box opens.
2. Make the following settings:
 - Network:** Select the (internal) network you want to masquerade.
 - Interface:** Select the (external) interface that is connected to the Internet.
 - Use Address:** If the interface you selected has more than one IP address assigned (see *Network >> Interfaces >> Additional Addresses*), you can define here which IP address is to be used for masquerading.
 - Comment (optional):** Add a description or other information about the masquerading rule.
3. Click **Save**.
The new masquerading rule appears on the *Masquerading* rule list.
4. Enable the masquerading rule.
Click the status icon to activate the masquerading rule.

To either edit or delete a masquerade rule, click the corresponding buttons.

Note – You need to allow traffic from the internal network to the Internet in the packet filter if you want your clients to access external servers.

DNAT/SNAT

Destination Network Address Translation (DNAT) and *Source Network Address Translation (SNAT)* are both special cases of NAT. With SNAT, the IP address of the computer which initiated the connection is rewritten, while with its counterpart DNAT, the destination addresses of data packets are rewritten. DNAT is especially useful when an internal network uses private IP addresses, but an administrator wants to make some services available to the outside.

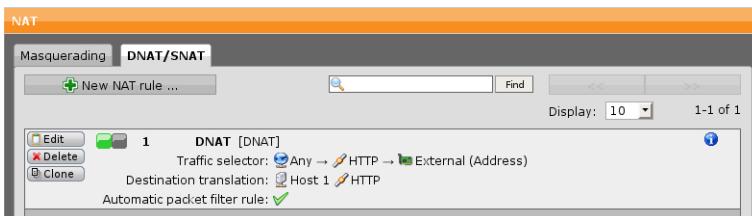


Figure 9.4 NAT Rule List

This is best demonstrated with an example. Suppose your internal network uses the address space 192.168.0.0/255.255.255.0 and a web server running at IP address 192.168.0.20 port 80 should be available to Internet-based clients. Because the 192.168. address space is private, the Internet-based clients cannot send packets directly to the web server. It is, however, possible for them to communicate with the external (public) address of the security system. DNAT can, in this case, take packets addressed to port 80 of the system's address and forward them to the internal web server.

Note – PPTP VPN Access is incompatible with DNAT.

In contrast to masquerading, which is dynamic, SNAT uses static address translation, that is, every internal address is translated to its own externally visible IP address.

Note – By default, port 443 (HTTPS) is used for the User Portal. If you plan to forward port 443 to an internal server, you need to change the TCP port of the User Portal to another value (e.g., 1443) on the *Management >> User Portal >> Advanced* tab.

Because DNAT is done before packet filtering, you must ensure that appropriate packet filter rules are defined. For more information, see *Network Security >> Packet filter >> Rules*.

To define a DNAT/SNAT rule, proceed as follows:

1. **On the *DNAT/SNAT* tab, click *New NAT Rule*.**

The *Create New NAT Rule* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for the NAT rule.

Group: Groups are useful to combine various NAT rules logically for better readability. A group can be any text string.

Position: The position number, defining the priority of the rule. Lower numbers have higher priority. Rules are matched in ascending order. Once a rule has matched, rules with a higher number will not be evaluated anymore.

Traffic Source: The original source address of the packet (this can be either a single host or an entire network).

Traffic Service: The original service type of the packet (consisting of source and destination ports as well as a protocol type).

Note – A traffic service can only be translated when the corresponding addresses are translated as well. In addition, a service can only be translated to another service when the two services use the same protocol.

Traffic Destination: The original destination address of the packet (this can be either a single host or an entire network).

NAT mode: Select the network address translation mode. The following modes are available:

- DNAT (Destination)
- SNAT (Source)
- Full NAT

Depending on your selection, various options will be displayed.

- If you have selected *DNAT*, choose a destination host/network and destination service, that is, the new destination address and service of the packet.
- If you have selected *SNAT*, choose a source host/network and source service, that is, the new source address and service of the packet.
- If you have selected *Full NAT*, choose a destination host/network plus destination service and a source host/network plus source service.

Log initial packets (optional): Select this option to write the initializing packet of a communication to the packet filter log. Whenever the NAT rule is used, you will then find a message in the packet filter log saying "Connection using NAT". This option works for stateful as well as stateless protocols.

Automatic Packet Filter Rules (optional): Select this option to automatically generate packet filter rules.

Comment (optional): Add a description or other information about the NAT rule.

3. Click **Save**.

The new rule appears on the NAT rule list.

4. Enable the NAT rule.

Click the status icon to activate the NAT rule.

To either edit or delete a NAT rule, click the corresponding buttons.

Intrusion Prevention

On the menu *Network Security >> Intrusion Prevention* you can define and manage IPS rules of the firewall. The *Intrusion Prevention system (IPS)* recognizes attacks by means of a signature-based IPS ruleset. The system analyzes the complete traffic and automatically blocks attacks before they can reach the network. The existing ruleset and attack patterns are updated through the pattern updates. New IPS attack pattern signatures are automatically imported to the ruleset as IPS rules.

Global

On the *Network Security >> Intrusion Prevention >> Global* tab you can activate the *Intrusion Prevention System (IPS)* of Astaro Security Gateway.

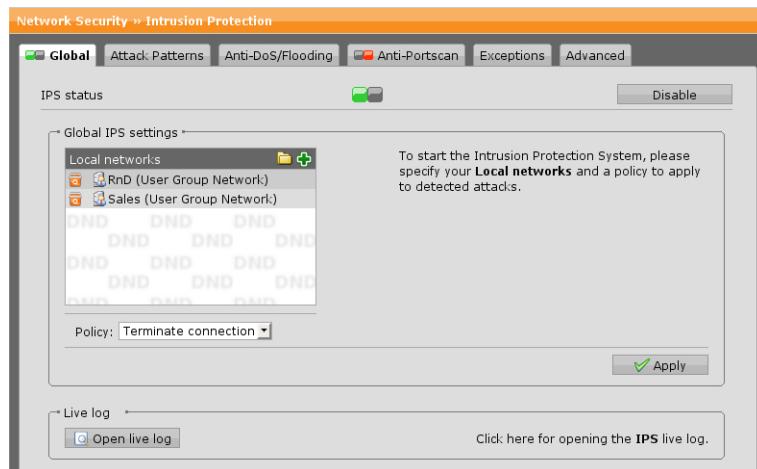


Figure 9.5 Configuring Intrusion Prevention

To enable IPS, proceed as follows:

1. Enable the intrusion prevention system.

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *Global IPS Settings* area becomes editable.

2. Make the following settings:

Local Networks: Select the networks that should be protected by the intrusion prevention system. If no local network is selected, intrusion prevention will automatically be deactivated and no traffic is monitored.

Policy: Select the security policy that the intrusion prevention system should use if a blocking rule detects an IPS attack signature.

- o **Drop Silently:** The data packet will be dropped without any further action.
- o **Terminate Connection:** A terminating data packet (*RST* for TCP and *ICMP Port Unreachable* for UDP connections) will be sent to both communication partners to close the connection.

Note – By default, *Drop Silently* is selected. There is usually no need to change this, especially as terminating data packets can be used by an alleged intruder to draw conclusions about the firewall.

3. Click **Apply**.

Your settings will be saved.

Open Live Log: The intrusion prevention live log can be used to monitor the selected IPS rules. Click the button to open the live log in a new window.

Attack Patterns

The *Network Security >> Intrusion Prevention >> Attack Patterns* tab contains IPS rules grouped according to common attack patterns. Attack patterns have been combined as follows:

- **Operating System Specific Attacks:** Attacks trying to exploit operating system related weaknesses.
- **Attacks Against Servers:** Attacks targeted at all sorts of servers (for example, web servers, mail servers, and so on).
- **Attacks Against Client Software:** Attacks aimed at client software such as web browsers, multimedia players, and so on.
- **Protocol Anomaly:** Attack patterns look out for network anomalies.
- **Malware:** Software designed to infiltrate or damage a computer system without the owner's informed consent (for example, trojans, DoS communication tools, and the like).

To improve performance, you should clear the checkboxes that do not apply to services or software employed in your local networks. For example, if you do not operate a web server in your local network, you can cancel the selection for *HTTP Servers*.

For each group, the following settings are available:

Action: By default, each rule in a group has an action associated with it. You can choose between the following actions:

- **Drop:** The default setting. If an alleged attack attempt has been determined, the causing data packets will be dropped.
- **Alert:** Unlike the *Drop* setting, critical data packets are allowed to pass the firewall but will create an alert message in the IPS log.

Intrusion Prevention

Global Attack Patterns Anti-Dos/Flooding Anti-Portscan Exceptions Advanced

This table shows the available IPS rule groups. To improve performance, you should deselect the groups that do not match services or software that you are running in your local networks. For each active group, three options can be set:

- Action:** By default, every rule in a group has a sensible default action. You can override these default by setting either Alert or Drop for a group.
- Add extra warnings:** When this option is activated, the group will also include rules which are used for warning-purposes only. These rules may potentially cause false alarms, so they are not included by default.
- Notify:** When this option is active, notifications will be sent for every hit in this group.

When you are finished making changes, click the **Apply** button on the bottom of the page.

Status / Group Name	Action	Options
<input checked="" type="checkbox"/> Operating system specific attacks (683 attacks, 1 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Windows (446 attacks, 1 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Linux (218 attacks)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Others (19 attacks)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Attacks against Servers (1703 attacks, 485 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> HTTP Servers (768 attacks, 359 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Common (156 attacks, 121 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Apache (11 attacks)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Microsoft IIS (142 attacks)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Other HTTP Servers (98 attacks)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Coldfusion (19 attacks, 25 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Frontpage (4 attacks, 34 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> PHP (148 attacks)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> CGI (190 attacks, 179 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Mail Servers (169 attacks, 16 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Exchange (2 attacks, 3 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Sendmail (18 attacks)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> POP3 (27 attacks, 1 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> IMAP (61 attacks, 1 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> SMTP (61 attacks, 11 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Database Servers (678 attacks, 42 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Microsoft SQL Server (121 attacks, 1 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Oracle (551 attacks, 29 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> MySQL (6 attacks, 12 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Misc Servers (88 attacks, 68 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> DNS (27 attacks)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> FTP (53 attacks, 31 warnings)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify
<input checked="" type="checkbox"/> Backup (Veritas, Arkeia, ARCServe) (2 attacks)	Drop	<input type="checkbox"/> Add extra warnings <input checked="" type="checkbox"/> Notify

Figure 9.6 Attack Patterns

Note – To change the settings for individual IPS rules, use the *Modified Rules* box on the *Intrusion Prevention >> Advanced* tab. A detailed list of IPS rules used in Astaro Security Gateway version 7 is available at the Astaro website²¹.

Add Extra Warnings: When this option is selected, each group will include additional rules increasing the IPS detection rate. Note that these rules are more general and vague than the explicit attack patterns and will therefore

²¹ <http://www.astaro.com/lists/ASGV7-IPS-rules.html>

likely produce more alerts. For that reason, the default action for these rules is Alert, which cannot be configured.

Notify: When this option is selected, a notification is sent to the administrator for every IPS event matching this group. Note that this option only takes effect if you have enabled the notification feature for the intrusion prevention system on the *Management >> Notifications >> Notifications* tab. In addition, what type of notification (i.e., e-mail or SNMP trap) is to be sent depends on the settings made there. Note further that it might take up to five minutes before changes of the notification settings will become effective.

Anti-DoS/Flooding

On the *Anti-DoS/Flooding* tab you can configure certain options aimed at defending *Denial of Service* (DoS) and *Distributed Denial of Service* (DDoS) attacks.

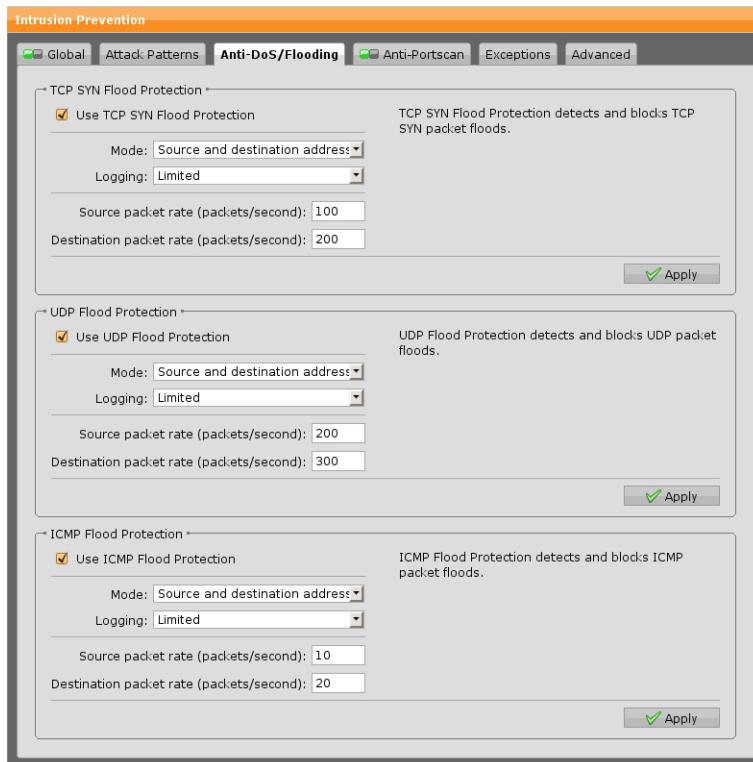


Figure 9.7 Configuring Flood Protection

Generally speaking, DoS and DDoS attacks try to make a computer resource unavailable for legitimate requests. In the simplest case, the attacker overloads the server with useless packets in order to overload its performance. Since a large bandwidth is required for such attacks, more and more attackers start using so-called *SYN flood attacks*, which do not aim at overloading the bandwidth, but at blocking the system resources. For this purpose, they send so-called SYN packets to the TCP port of the service often with a forged sender address, thus causing the server to spawn a half-open connection by sending back a TCP/SYN-ACK packet, and waiting for an TCP/ACK packet in response from the sender address. However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests.

Such attacks, however, can be prevented by limiting the amount of SYN (TCP), UDP, and ICMP packets being sent into your network over a certain period of time.

TCP SYN Flood Protection

To enable SYN (TCP) flood protection, proceed as follows:

1. On the *Anti-DoS/Flooding* tab, select the checkbox **Use TCP SYN Flood Protection**.
2. Make the following settings:

Mode: The following modes are available:

- **Both Source and Destination Addresses:** Select this option if you want to drop SYN packets that match both source and destination IP address. First, SYN packets are filtered that match the source IP address. Second, if there are still too many requests they will additionally be filtered according to the destination IP address. This mode is set as default.
- **Destination Address Only:** Select this option if you want to drop SYN packets according to the destination IP address only.
- **Source Address Only:** Select this option if you want to drop SYN packets according to the source IP address only.

Logging: This option lets you select the log level. The following levels are available:

- **Off:** Select this log level if you want to turn logging completely off.
- **Limited:** Select this log level to limit logging to five packets per seconds. This level is set as default.
- **Everything:** Select this log level if you want verbose logging for all SYN (TCP) connection attempts. Note that SYN (TCP) flood attacks may lead to extensive logging.

Source Packet Rate: Here you can specify the rate of packets per second that is allowed for source IP addresses.

Destination Packet Rate: Here you can specify the rate of packets per second that is allowed for destination IP addresses.

Note – It is important to enter reasonable values here, for if you set the rate too high, your webserver, for instance, might fail because it cannot deal with such an amount of SYN (TCP) packets. On the other hand, if you set the rate too low, your firewall might show some unpredictable behavior by blocking regular SYN (TCP) requests. Reasonable settings for every system heavily depend on your hardware. Therefore, replace the default values by numbers that are appropriate for your system.

3. Click **Apply**.

Your settings will be saved.

UDP Flood Protection

UDP Flood Protection detects and blocks UDP paket floods.

The configuration of *UDP Flood Protection* is identical to *TCP SYN Flood Protection*.

ICMP Flood Protection

ICMP Flood Protection detects and blocks ICMP paket floods.

The configuration of *ICMP Flood Protection* is identical to *TCP SYN Flood Protection*.

Anti-Portscan

The *Network Security >> Intrusion Prevention >> Anti-Portscan* tab lets you configure general portscan detection options.

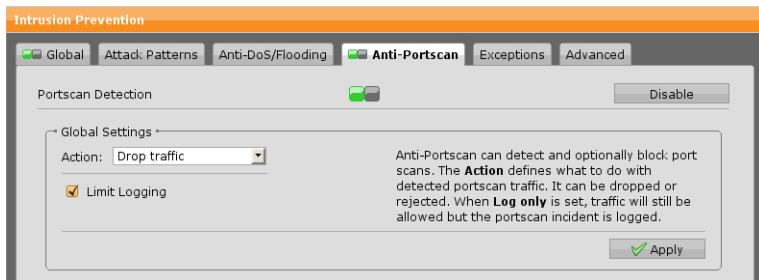


Figure 9.8 Configuring Portscan Protection

Portscans are used by hackers to probe secured systems for available services: In order to intrude into a system or to start a *Denial of Service* (DoS) attack, attackers need information on network services. If this information is available, attackers might take advantage of the security deficiencies of these services. Network services using the TCP and UDP Internet protocols can be accessed via special ports and this port assignment is generally known, for example the SMTP service is assigned to the TCP Port 25. Ports that are used by the services are referred to as open, since it is possible to establish a connection to them, whereas unused ports are referred to as closed; every attempt to connect with them will fail. Attackers try to find the open ports with the help of a particular software tool, a port scanner. This program tries to connect with several ports on the destination computer. If it is successful, the tool displays the relevant ports as open and the attackers have the necessary information, showing which network services are available on the destination computer.

Since there are 65535 distinct and usable port numbers for the TCP and UDP Internet protocols, the ports are scanned at very short intervals. If the firewall detects an unusually large number of attempts to connect to services, especially if these attempts come from the same source address, the firewall is most likely being port scanned. If an alleged attacker performs a scan of hosts or services on your network, the portscan detection feature will recognize this. As an option, further portscans from the same source address can be blocked automatically.

Technically speaking, a portscan is detected when a detection score of 21 points in a time range of 300 ms for one individual source IP address is exceeded. The detection score is calculated as follows:

- Scan of a TCP destination port less than 1024 = 3 points
- Scan of a TCP destination port greater or equal 1024 = 1 point
- Scan of ports 11, 12, 13, 2000 = 10 points

To enable portscan detection, proceed as follows:

1. **On the Anti-Portscan tab, enable Portscan Detection.**

You can either click the status icon or the *Enable* button.

The status icon turns green and the *Global Settings* area becomes editable.

2. **Make the following settings:**

Action: Select one of the following actions:

- **Log Event Only:** No measures are taken against the portscan. The event will be logged only.
- **Drop Traffic:** Further packets of the portscan will be silently dropped. A port scanner will report these ports as filtered.
- **Reject Traffic:** Further packets of the portscan will be dropped and an ICMP "destination unreachable/port unreachable" response will be sent to the originator. A port scanner will report these ports as closed.

Limit Logging: Enable this option to limit the amount of log messages. A portscan detection may generate many logs while the portscan is being carried out. For example, each SYN packet that is regarded as belonging to the portscan will generate an entry in the packet filter log. Selecting this option will restrict logging to five lines per second.

3. **Click *Apply*.**

Your settings will be saved.

Exceptions

On the *Network Security >> Intrusion Prevention >> Exceptions* tab you can define source and destination networks that should be excluded from intrusion prevention.

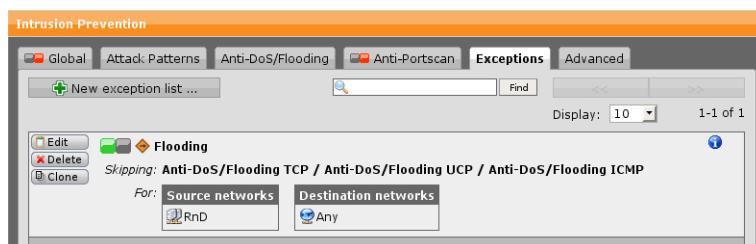


Figure 9.9 Intrusion Prevention Exceptions List

To create an exception list, proceed as follows:

1. **On the Exceptions tab, click New Exception List.**

The *Create Exception List* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for this exception.

Skip Features: Select the security checks that should be skipped:

- **Intrusion Prevention:** When you select this option, the IPS of Astaro Security Gateway will be disabled.
- **Anti-Portscan:** Selecting this options disables the protection from attacks aimed at searching your network hosts for open ports.
- **Anti-DoS/Flooding TCP:** Once selected, the protection from TCP SYN flooding attacks will be disabled.
- **Anti-DoS/Flooding UDP:** Once selected, the protection from UDP flooding attacks will be disabled.
- **Anti-DoS/Flooding ICMP:** Once selected, the protection from ICMP flooding attacks will be disabled.

Source Networks: Select the source networks that should be exempt from the security checks of this exception rule.

When selecting this option, the *Source Networks* text box opens.

Destination Networks: Select the destination networks that should be exempt from the security checks of this exception rule.

When selecting this option, the *Destination Networks* text box opens.

Comment (optional): Add a description or other information about the exception.

3. **Click Save.**

The new exception list appears on the *Exceptions* list.

To either edit or delete an exception, click the corresponding buttons.

Note – If you want to except intrusion prevention for packets with the destination address of the firewall, selecting *Any* in the *Destination Networks* box will not succeed. You must instead select an interface definition of the firewall that contains the firewall's IP address, for example, *Internal (Address)* if you want to exclude intrusion prevention for the firewall's internal address.

Advanced

On the *Network Security >> Intrusion Prevention >> Advanced* tab you can configure manual modifications to each IPS rule overwriting the default policy, which is taken from the attack pattern groups. Such modifications should be configured by experienced users only.

To create a modified rule, proceed as follows:

1. In the **Modified Rules** box, click the plus icon.

The *Modify Rule* dialog box opens.

2. Make the following settings:

Rule ID: Enter the ID of the rule you want to modify. To look up the rule ID, go to the list of IPS rules at the Astaro Website (available both in HTML²² and XML²³ format). In addition, they can either be determined from the IPS log or the IPS report.

Disable this Rule: When you select this option, the rule of the respective ID will be disabled.

If do *not* select this option, however, the following two options are available:

- **Disable Notifications:** Selecting this option will not trigger a notification in case the rule in question was applied.
- **Action:** The action each rule is associated with it. You can choose between the following actions:
 - **Drop:** If an alleged attack attempt has been determined, the causing data packets will be dropped.
 - **Alert:** Unlike the *Drop* setting, critical data packets are allowed to pass the firewall but will create an alert message in the IPS log.

3. Click **Save**.

The rule appears in the *Modified Rules* box. Please note that you also need to click *Apply* on the bottom of the page to commit the changes.

²² <http://www.astaro.com/lists/ASGV7-IPS-rules.html>

²³ <http://www.astaro.com/lists/ASGV7-IPS-rules.xml>

Note – If you add a rule ID to the *Modified Rules* box and set the action to *Alert*, for example, this modification will only take effect if the group to which the rule belongs is enabled on the *Attack Patterns* tab. If the corresponding attack pattern group is disabled, modifications to individual IPS rules will have no effect.

Performance Tuning

In addition, to increase the performance of the intrusion prevention system and to minimize the amount of false positive alerts, you can limit the scope of IPS rules to only some of your internal servers. For example, suppose you have activated the *HTTP Servers* group on the *Attack Patterns* tab and you have selected a particular HTTP server here. Then, even if the intrusion prevention system recognizes an attack against an HTTP server, the associated action (*Drop* or *Alert*) will only be applied if the IP address of the affected server matches the IP address of the HTTP server selected here.

You can limit the scope of IPS rules for the following server types:

- **HTTP:** All attack pattern groups subsumed under *HTTP Servers*
- **DNS:** Attack pattern group *DNS*
- **SMTP:** Attack pattern groups *Exchange* and *Sendmail*
- **SQL:** All attack pattern groups subsumed under *Database Servers*

Server Load Balancing

With the server load balancing function you can distribute incoming connections (e.g., SMTP or HTTP traffic) to several servers behind the firewall. Balancing is based on the source IP address with a persistence time of one hour. If the interval between two requests from the same source IP address exceeds that interval, the balancing is redetermined. The traffic distribution is based on a simple round-robin algorithm.

All servers from the server pool are monitored either by ICMP ping, TCP connection establishment, or HTTP/S requests. In case of a failure the affected server is not used anymore for distribution, any possible source IP persistence is overruled.

Note – A return code of HTTP/S requests must either be 1xx Informational, 2xx Success, 3xx Redirection, or 4xx Client Error. All other return codes are taken as failure.

Balancing Rules

On the *Network Security >> Server Load Balancing >> Balancing Rules* tab you can create load balancing rules for Astaro Security Gateway Software.



Figure 9.10 Balancing Rule List

To set up a load balancing rule, proceed as follows:

1. On the **Balancing Rules** tab, click **New Load Balancing Rule**.

The *Create New Load Balancing Rule* dialog box opens.

2. Make the following settings:

Service: Select the network service you want to balance.

Virtual Server: The original target host of the incoming traffic. Typically, the address will be the same as the firewall's external address.

Real Servers: The hosts that will in turn accept traffic for the service.

Check Type: Select either *Ping* (ICMP Ping), *TCP* (TCP connection establishment), *HTTP Host* (HTTP requests), or *HTTPS Hosts* (HTTPS requests) for service monitoring. For HTTP and HTTPS requests enter additionally a *Check URL*, which can either be with or without hostname, e.g. `index.html` or `www.example.com/index.html`.

Check Interval: Enter a check interval in seconds. The default is 15 seconds, i.e. every 15 seconds the health status of all real servers is checked.

Automatic Packet Filter Rules: Select this checkbox to automatically generate packet filter rules. These rules allow forwarding traffic from any host to the real servers.

Comment (optional): Add a description or other information about the load balancing rule.

3. Click Save.

The new rule appears on the *Balancing Rules* list. It is disabled by default.

4. Enable the load balancing rule.

Click the red status icon to enable the rule.

The status icon turns green.

To either edit or delete a load balancing rule, click the corresponding buttons.

Example: Suppose that you have two HTTP servers in your DMZ with the IP addresses 192.168.66.10 and 192.168.66.20, respectively. Assumed further you want to distribute HTTP traffic arriving on the external interface of your firewall equally to both servers. To set up a load balancing rule, select or create a host definition for each server. You may call them *http_server_1* and *http_server_2*. Then, in the *Create New Load Balancing Rule* dialog box, select *HTTP* as *Service*. In addition, select the external address of the firewall as *Virtual Server*. Finally, put the host definitions into the *Real Servers* box.

Advanced

The tabs of the *Network Security >> Advanced* menu let you configure additional network security features such as a generic proxy, SOCKS proxy, and IDENT Reverse proxy.

Generic Proxy

A generic proxy, also known as a port forwarder, combines both features of DNAT and masquerading, forwarding all incoming traffic for a specific service to an arbitrary server. The difference to standard DNAT, however, is that a generic proxy also replaces the source IP address of a request with the IP address of the interface for outgoing connections. In addition, the destination (target) port number can be changed as well.

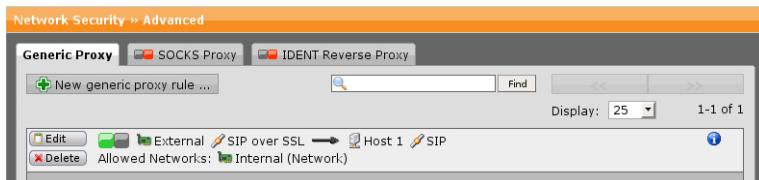


Figure 9.11 Generic Proxy Rule List

To add a generic proxy rule, proceed as follows:

1. On the **Generic Proxy** tab, click **New Generic Proxy Rule**.

The *Create New Generic Proxy Rule* dialog box opens.

2. Make the following settings:

Interface: Select the interface for incoming connections.

Service: Select the service definition of the traffic to be proxied.

Host: Select the target host where the traffic should be forwarded to.

Service: Select the target service of the traffic to be proxied.

Allowed Networks: Select the networks to which port forwarding should be applied.

Comment (optional): Add a description or other information about this generic proxy rule.

3. Click **Save**.

The new rule appears on the *Generic Proxy* rule list.

4. Activate the generic proxy rule.

Click the status icon to enable the rule.

The rule is now active.

To either edit or delete a rule, click the corresponding buttons.

SOCKS Proxy

SOCKS is a versatile Internet protocol that allows client-server applications to transparently use the services of a network firewall. It is used by many client applications behind a firewall to communicate with hosts on the Internet. Examples are IRC/Instant Messaging clients, FTP clients, and Windows SSH/Telnet clients. Those clients behind a firewall wanting to access exterior servers connect to a SOCKS proxy server instead. This proxy server controls the eligibility of the client to access the external server and passes the request on to the server. Your client application must explicitly support the SOCKS 4 or SOCKS 5 protocol versions.

The default port for SOCKS is 1080. Almost all clients have implemented this default port setting, so it normally does not have to be configured. The differences between SOCKS and NAT are that SOCKS also allows "bind" requests (listening on a port on behalf of a client—a feature which is supported by very few clients only) and that SOCKS 5 allows user authentication.

When enabling the SOCKS proxy, you must define one or more networks which should have access to the proxy. When you require user authentication, you can also select the users or groups that should be allowed to use the SOCKS Proxy.

Note – Without user authentication, the SOCKS proxy can be used with both the SOCKS 4 and SOCKS 5 protocols. When user authentication is selected, only SOCKS 5 will work. If you want the proxy to resolve hostnames in SOCKS 5 mode, you must also activate the DNS proxy, because otherwise DNS resolution will fail.

To configure the SOCKS proxy, proceed as follows:

1. **On the *SOCKS Proxy* tab, enable the *SOCKS proxy*.**

You can either click the status icon or the *Enable* button.

The status icon turns green and the *SOCKS Proxy Options* area becomes editable.

2. **Make the following settings:**

Allowed Networks: Select the networks that should be allowed to use the SOCKS proxy.

Enable User Authentication: If you select this option, users must provide a username and password to log in to the SOCKS proxy. Because only SOCKS 5 supports user authentication, SOCKS 4 is automatically disabled.

Allowed Users: Select the users or groups that should be allowed to use the SOCKS proxy.

3. **Click *Apply*.**

Your settings will be saved.

IDENT Reverse Proxy

The IDENT protocol is used by remote servers for a simple verification of the identity of accessing clients. Although this protocol is unencrypted and can easily be spoofed, many services still use (and sometimes require) the IDENT protocol.

To configure the IDENT relay, proceed as follows:

1. **On the *IDENT Reverse Proxy* tab, enable the *IDENT relay*.**

You can either click the status icon or the *Enable* button.

The status icon turns green and the *Global Settings* area becomes editable.

2. **Make the following settings:**

Forward to Internal Hosts (optional): Since IDENT queries are not covered by the firewall's connection tracking, they will get "stuck" if masquerading is used. You can select the *Forward to Internal Hosts* option to

pass on IDENT queries to masqueraded hosts behind the firewall. Note that the actual IP connection will not be forwarded. Instead, the firewall will in turn ask the internal client for an IDENT reply and will forward that string to the requesting server. This scheme will work with most "mini-IDENT" servers built into popular IRC and FTP clients.

Default Response: The firewall offers support for answering IDENT requests when you enable the IDENT relay. The system will always reply with the string entered in the *Default Response* box, regardless of the local service that has initiated the connection.

3. **Click *Apply*.**

Your settings will be saved.

Web Security

This chapter describes how to configure basic web security features of Astaro Security Gateway.

The following topics are included in this chapter:

- HTTP/S Proxy
- HTTP/S Profiles
- FTP Proxy

The *Web Security Statistics* page in WebAdmin provides an overview of the most surfed domains according to time and traffic as well as for the top users surfing. In addition, the top blocked website categories are shown. Each of the sections contains a *Details* link. Clicking the link redirects you to the respective *Reporting* section of WebAdmin, where you can find more statistical information.

Note – The collection of web surfing data is session-based. To achieve good approximations all data for top domains and users is gathered as follows: each web request is logged by taking the traffic volume and the duration between requests into account. If for a period of five minutes of inactivity no requests are recorded for either a user or a domain, the session is considered closed. To take into account that users might still view a web page within five minutes of inactivity, one minute is always added to the *Time Spent* values. Note further that reporting data is updated every 15 minutes.

When clients try to request invalid URLs, the proxy will log the request but will not be able to serve it. Those links will be counted with error on the *Web Security Statistics* page. This is not an error of the reporting or the HTTP/S proxy; in most cases, those errors occur because invalid or malformed links are placed in web content by the page creator.

HTTP/S

The tabs of the *HTTP/S* menu allow you to configure Astaro Security Gateway Software as an HTTP/S caching proxy. In addition to simple caching services, the *HTTP/S* of Astaro Security Gateway features a rich set of web filtering techniques for the networks that are allowed to use its services. This includes preventing virus and spyware infections by means of two different virus scanning engines with constantly updated signature databases and spyware filtering techniques that protects both inbound and outbound traffic. Moreover, Astaro Security Gateway can control access to various web pages by employing sophisticated website categorization, using the world's largest real-time URL database.

Global

On the *Web Security >> HTTP/S >> Global* tab you can make the global settings for the HTTP/S proxy.

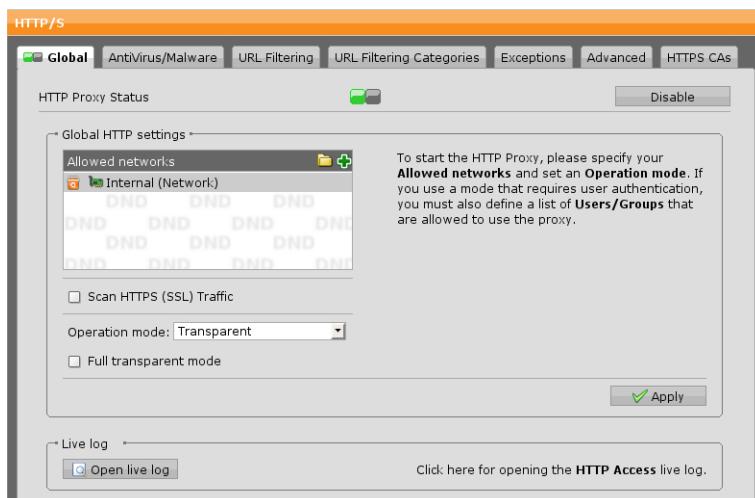


Figure 10.1 Global HTTP Settings

To configure the HTTP/S proxy, proceed as follows:

1. **On the *Global* tab, enable the HTTP proxy.**

You can either click the status icon or the *Enable* button.

The status icon turns green and the *Global HTTP Settings* area becomes editable.

2. Select the allowed networks.

Select the networks that should be allowed to use the HTTP proxy. By default, the HTTP proxy listens for client requests on TCP port 8080 and allows any client from the networks listed in the *Allowed Networks* box to connect.

3. Scan HTTPS (SSL) Traffic

Select the checkbox to not only scan HTTP traffic but HTTPS traffic, too.

4. Select a mode of operation.

Note that when you select an operation mode that requires user authentication, you should also select the users and groups that shall be allowed to use the HTTP proxy. However, if no users or groups are selected, every user who has successfully authenticated against the directory service can use the HTTP proxy.

The following modes of operation are available:

- **Standard:** In standard mode, the HTTP proxy will listen for client requests on port 8080 by default and will allow any client from the networks listed in *Allowed Networks* box to connect. When used in this mode, clients must have specified the HTTP proxy in their browser configuration.
- **Active Directory SSO:** Select when you have configured *Active Directory Single Sign-On (SSO)* on the *Users >> Authentication >> Servers* tab. This has the effect that NTLM user authentication will be used to authenticate clients. Note that this is only guaranteed to work with Internet Explorer. When used in this mode, clients must have specified the HTTP proxy in their browser configuration. You can select or add users and/or groups to the *Users/Groups* text box who are to be allowed to use the proxy.
- **Apple OpenDirectory SSO:** Select when you have configured *LDAP* on the *Users >> Authentication >> Servers* tab and you are using Apple OpenDirectory. Additionally, you have to upload a MAC OS X Single Sign-On Kerberos keyfile on the *Web Security >> HTTP/S >> Advanced* tab for the proxy to work properly. When the HTTP proxy is used in this mode, clients must have specified the HTTP proxy in their browser configuration. You can select or add users and/or groups to the

Users/Groups text box who are to be allowed to use the proxy. Note that the Safari browser does not support SSO.

- **Basic User Authentication:** In *Basic User Authentication* mode, each client must authenticate itself against the proxy before using it. For more information about which authentication methods are supported, see *Users >> Authentication*. When used in this mode, clients must have specified the HTTP proxy in their browser configuration. You can select or add users and/or groups to the *Users/Groups* text box who are to be allowed to use the proxy.
- **eDirectory SSO:** Select when you have configured eDirectory on the *Users >> Authentication >> Servers* tab. When used in this mode, clients must have specified the HTTP proxy in their browser configuration. You can select or add users and/or groups to the *Users/Groups* text box who are to be allowed to use the proxy.

Note – For eDirectory and Active Directory Single-Sign-On (SSO) modes, the proxy caches accessing IP addresses and credentials for up to fifteen minutes, for Apple OpenDirectory SSO it caches only the group information. This is done to reduce the load on the authentication servers. However it also means that changes to users, groups, or the login status of accessing users may take up to fifteen minutes to be reflected by the HTTP/S proxy.

- **Transparent:** In transparent mode, all connections made by client browser applications on port 80 (port 443, respectively, if SSL is used) are intercepted and redirected to the proxy without client-side configuration. The client is entirely unaware of the proxy server. The advantage of this mode is that no additional administration or client-side configuration is necessary, the disadvantage however is that only HTTP (port 80) requests can be processed. Thus, when you select *Transparent* as mode, the client's proxy settings will become ineffective.

Full Transparent Mode (optional): Select the checkbox *Full Transparent Mode* to preserve the client source IP instead of replacing it by the firewall's IP. This is useful if your clients use public IP addresses that should not be disguised by the proxy.

Note – In transparent mode, the proxy will strip NTLM authentication headers from HTTP requests. Furthermore, the proxy cannot handle FTP requests in this mode. If your clients want to access such services, you must open the port (21) in the packet filter. Note further that some web servers transmit some data, in particular streaming video and audio, over a port different from port 80. These requests will not be noticed when the proxy operates in transparent mode. To support such traffic, you must either use a different mode or enter an explicit packet filter rule allowing them.

- **Transparent with Authentication:** Use this mode to force users to authenticate while the proxy is working transparently. When users open a website for the first time, they will be presented an authentication user-portal-like webpage where they have to fill in username and password. This mode allows for username-based tracking, reporting, and surfing without client-side browser configuration. Moreover, you can enable a disclaimer that is additionally displayed on that dialog window and needs to be accepted by users to be able to go on. For more information on the disclaimer, please refer to chapter *Management >> Customization >> HTTP/S Proxy*. You can select or add users and/or groups to the *Users/Groups* text box who are to be allowed to use the proxy.

5. Click **Apply**.

Your settings will be saved.

Important Note – When SSL scanning is enabled in combination with the transparent mode, certain SSL connections are destined to fail, e.g. SSL VPN tunnels. To enable SSL VPN connections, add the respective target host to the *Transparent Mode SkipList* (see *Web Security >> HTTP/S >> Advanced*).

AntiVirus/Malware

On the *Web Security >> HTTP/S >> AntiVirus/Malware* tab you can configure those options aiming at protecting your network from web traffic that carries harmful and dangerous content such as viruses, worms, or other malware.

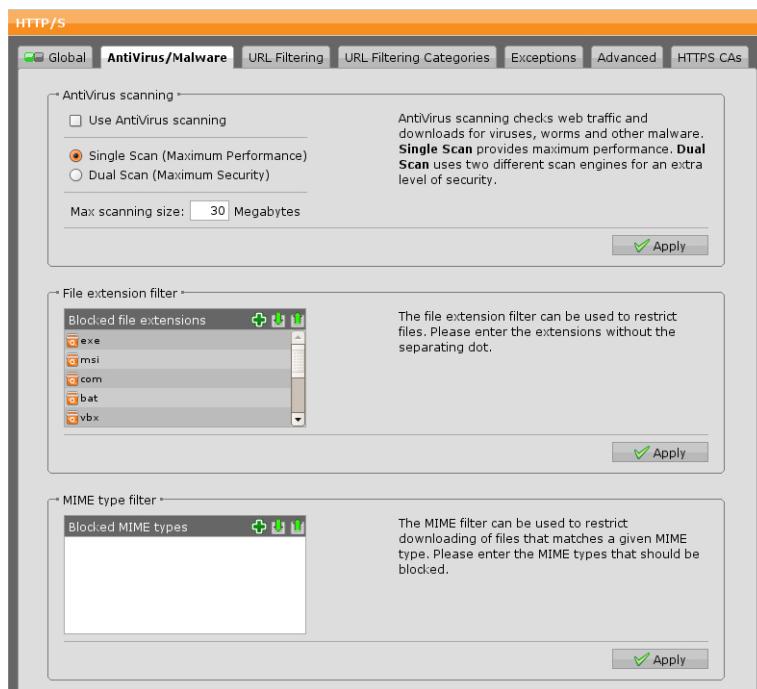


Figure 10.2 Configuring HTTP Proxy AntiVirus and Malware Settings

AntiVirus Scanning

Select the option *Use AntiVirus Scanning* to have inbound and outbound web traffic scanned. Astaro Security Gateway features several antivirus engines for best security.

- **Single Scan:** Default setting; provides maximum performance.
- **Dual Scan:** Provides maximum recognition rate by scanning all web traffic twice using different virus scanners.

Max Scanning Size: Specify the maximum size of files to be scanned by the antivirus engine(s). Files exceeding this size will be exempt from scanning. Click *Apply* to save your settings.

File Extension Filter

This feature filters certain types of files based on their extensions (e.g., executable binaries) from web traffic that have a file extension listed in the *Blocked File Extensions* box. You can add additional file extensions or delete file extensions that are not to be blocked. To add a file extension, click the plus icon

in the *Blocked File Extensions* box and enter the file extension you want to block, for example exe (without the delimiting dot). Click *Apply* to save your settings.

Note – Encrypted zip archives cannot be scanned for malicious content and will pass through the virus scanner. To protect your network from malware included in encrypted zip files you might want to consider blocking the zip file extension altogether.

MIME Type Filter

To add a MIME type that shall be blocked, click the plus icon in the *Blocked MIME Types* box and enter the MIME type (e.g., image/gif). It is possible to use wildcards (*) here, e.g. audio/*.

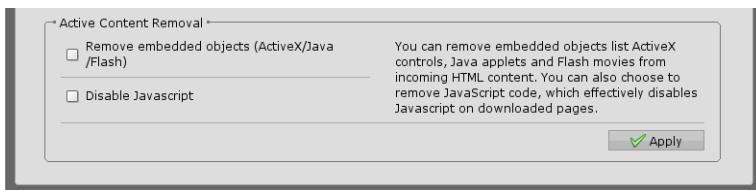


Figure 10.3 Configuring Active Content Removal Settings

Active Content Removal

In the *Active Content Removal* area you can configure the automatic elimination of specific web content such as embedded objects (e.g., multimedia files) in web pages. You can make the following settings:

- **Remove Embedded Objects:** When selected, this feature will remove all <OBJECT> tags from HTML pages, stripping off dynamic content such as ActiveX, Flash, or Java from incoming HTTP traffic.
- **Disable JavaScript:** When selected, this feature will disable all <SCRIPT> tags in HTML pages, resulting in the deactivation of functions that are embedded in or included from HTML pages.

URL Filtering

On the *Web Security >> HTTP/S >> URL Filtering* tab you can configure your default settings for controlling access to certain kinds of websites.

Note – The whitelist is always queried first, i.e. each website request is compared with the whitelist and if no match can be found the request is compared to the blacklist. If a match with the blacklist is found, the website is blocked.

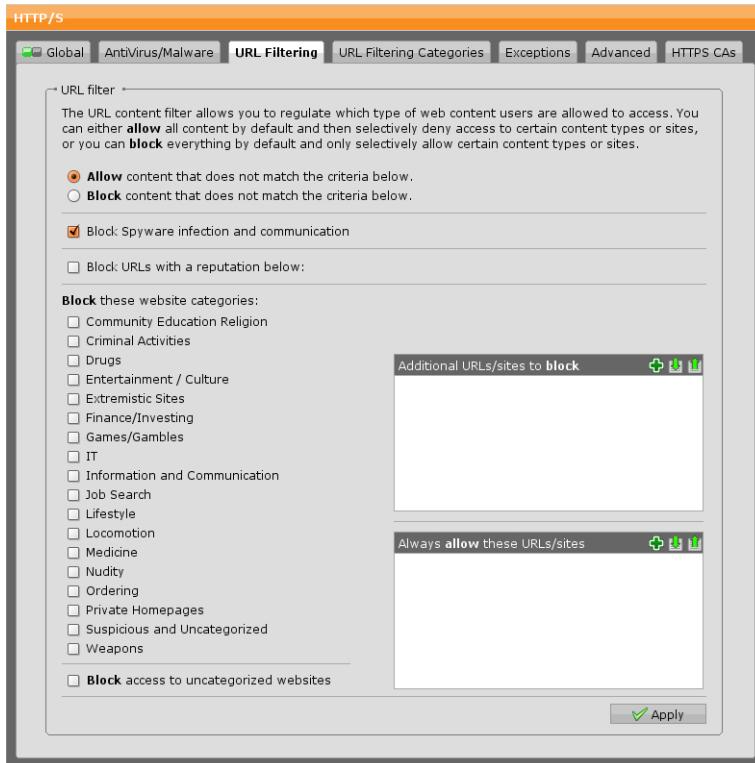


Figure 10.4 Configuring the URL Filtering

You can make the following settings:

- **Allow/Block selection:** Decide whether your selection of website categories should be allowed or blocked. The following options are available:

- **Allow Content that Does not Match the Criteria Below:** If this option is selected, your selection of website categories will be blocked while all other categories not selected will be allowed.
- **Block Content that Does not Match the Criteria Below:** If this option is selected, all website categories except the ones you selected will be blocked.

The default option is *Allow*. When you switch to *Block*, note that the options below are subsequently "inverted" in their meaning which is displayed by a change of wording from *Block* to *Allow* and vice versa, respectively.

Note – For accessing the categorization database, TCP port 6000 or TCP port 80 needs to be open in upstream firewalls. If you have a parent proxy configured, all requests to the database will be sent through the parent proxy.

- **Block Spyware Infection and Communication:** Spyware is malicious software that can probe systems and reports user behavior to an advertiser without the user's knowledge. Selecting this option will detect and block spyware on the way from the server to the client. Doing this would prevent computers within your network from getting infected by new spyware. Moreover, activating this feature will detect and block traffic from already installed spyware applications. In doing so, gathered user information will no longer be submitted to the Internet. Note that this option is only available if the first option on the page is set to *Allow*.

Note – The spyware category cannot be assigned to any of the 18 available groups, therefore protection from spyware purveyors can only be enabled by selecting the *Block Spyware Infection and Communication* checkbox.

- **Block URLs with a Reputation Below a Threshold of:** Websites can be classified as either *Trusted*, *Neutral*, *Suspicious*, or malicious, the latter not being listed (since it would allow for all kind of sites which is equivalent to not using the threshold option at all). Unclassified websites are referred to as *Unverified*. You can determine which reputation a website must have to be accessible from your network. Websites below the selected threshold will be blocked. Note that this option is only available if the first option

on the page is set to *Allow*. For more information on website reputations please refer to <http://www.trustedsource.org>.

- **Block these Website Categories:** Select the website categories that should be blocked. Note that this option changes to *Allow these Website Categories* if the first option on the page is set to *Block*. The mapping between the website categories to be selected here and their underlying subcategories can be changed on the *Web Security >> HTTP/S >> URL Filtering Categories* tab.

Note – If you are of the opinion that a website is wrongly categorized, you can use Astaro's URL report form²⁴ to suggest new categories.

- **Block Access to Uncategorized Websites:** Enabling this option will prevent the browser from opening websites of unknown content. This function can be considered as a fallback security mechanism in case a potentially unwanted website has not yet been categorized as such.
One benefit of this function is to protect the user from so-called *phishing* attacks. Usually, phishing e-mails contain suspicious links to faked websites, tricking the user into revealing personal and confidential information. If not already classified as harmful, those links are either of category *Uncategorized* or *Suspicious*. By selecting this option, those categories will be blocked. Thus, even if a phishing message has been delivered, the user won't be able to open the fraudulent URL.
Note that this option changes to *Allow Access to Uncategorized Websites* if the first option on the page is set to *Block*.
- **Additional URLs/Sites to Block:** If you want to block a specific URL or website regardless of its category, enter it here. This has the effect that websites listed here can be blocked even if they belong to a category you want to allow. Regular expressions are allowed here (e.g. `^https?://.*wikipedia.org`). To block exactly one URL enter the complete URL (e.g. `http://www.wikipedia.org`). Note that expressions such as `wikipedia.org` do not only match the URL but also search results and parts of similar URLs which may lead to unwanted blocking behavior.

²⁴ <http://www.astaro.com/tool/urlreport>

Note that this option changes to *Additional URLs/Sites to Allow* if the first option on the page is set to *Block*.

- **Always Allow these URLs/Sites:** If you explicitly want to allow a specific URL or website regardless of its category or an entry in the block list, enter it here. Regular expressions are allowed here (e.g. ^https://.*wikipedia.org). To block exactly one URL enter the complete URL (e.g. http://www.wikipedia.org). Note that expressions such as wikipedia.org do not only match the URL but also search results and parts of similar URLs which may lead to unwanted blocking behavior.
Note that this option changes to *Always Block these URLs/Sites* if the first option on the page is set to *Block*.

URL Filtering Categories

Here you can customize the mapping of website categories to category groups, which can be selected on the *Web Security >> HTTP/S >> URL Filtering* tab. Astaro Security Gateway can identify and block access to 60 different categories of websites. Sophisticated URL classification methods ensure accuracy and completeness in identifying questionable websites. If a user requests a web page that is not included in the database, the URL is sent to the web crawlers and classified automatically.

Note – If you are of the opinion that a website is wrongly categorized, you can use Astaro's URL report form²⁵ to suggest new categories.

To assign website categories to a category group, proceed as follows:

1. **Click *Edit* in the category group you want to edit.**
The *Edit Filter Category* dialog box opens.
2. **Select the categories.**
Select or clear the checkboxes of the categories you want to add to or remove from the group.
3. **Click *Save*.**
The group will be updated with your settings.

Alternatively, you can also create a new filter category. Proceed as follows:

²⁵ <http://www.astaro.com/tool/urlreport>

1. Click the **New Filter Category** button on the top of the page.

The *Create Filter Category* dialog box opens.

2. Enter a name.

Enter a descriptive name for the new filter category.

3. Select the categories.

Select the checkboxes of the categories you want to add to the group.

4. Click Save.

The group will be updated with your settings.

To either edit or delete a category, click the corresponding buttons.

Exceptions

On the *Web Security >> HTTP/S >> Exceptions* tab you can define whitelist client networks, users/groups, and domains. All entries contained in these lists can be excluded from certain web security services.

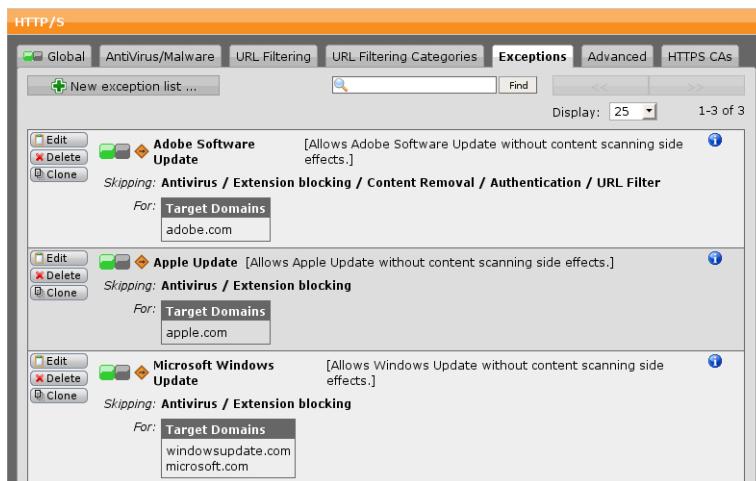


Figure 10.5 HTTP Proxy Exceptions List

To create an exception, proceed as follows:

1. On the **Exceptions** tab, click **New Exception List**.

The *Create Exception List* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for this exception.

Skip Features: Select the security checks that should be skipped:

- **Authentication:** If the HTTP proxy runs in *Authentication* mode, you can skip authentication for the source hosts/networks, target domains, or users/groups.
- **Caching:** Select to disable caching for specific domains or source hosts/networks.
- **AntiVirus:** Select to disable virus scanning, which checks messages for unwanted content such as viruses, trojan horses and the like.
- **Extension Blocking:** Select to disable the file extension filter, which can be used to block content that contains certain types of files based on their extensions.
- **MIME Type Blocking:** Select to disable the MIME type filter, which can be used to block content that has a certain MIME type.
- **URL Filter:** Select to disable the URL filter, which controls the access to certain kinds of websites.
- **Content Removal:** Select to bypass the removal of special content in web pages such as embedded objects (e.g., multimedia files) or JavaScript.
- **SSL Scanning:** Select to skip SSL scanning for the webpage in request. This is useful with online banking websites or with websites that do not play well with SSL interception. Note that for technical reasons this option does not work for any Transparent proxy mode. With Transparent mode, use the Transparent Skiplist instead (see section *Advanced*). In Standard mode, exceptions can only be made based on the destination host or IP address depending on what the client sends. With exceptions based on Categories, instead of the whole URL, only the hostname will be classified.

- **Certificate Trust Check:** Select to skip the trust check of the HTTPS server certificate.
- **Certificate Date Check:** Select to skip the check of whether the HTTPS certificate's date is valid.

The following two options are useful if there are persons or members of e.g. a works council whose activities must not be logged at all:

- **Accessed Pages:** Select to not log pages that have been accessed. Those page requests will also be excluded from reporting.
- **Blocked Pages:** Select to not log pages that have been blocked. Those page requests will also be excluded from reporting.

For These Source Hosts/Networks: Select to add source hosts/networks that should be exempt from the security checks of this exception rule. Enter the respective hosts or networks in the *Source Hosts/Networks* dialog box that opens after selecting the checkbox.

Matching These URLs: Select this checkbox to add target domains that should be exempt from the security checks of this exception rule. Add the respective domains to the *Target Domains* dialog box that opens after selecting the checkbox. Example: ^https?://[^.]*\domain.com matches HTTP(S) connections to all subdomains of the domain.

These Users/Groups: Select checkbox to add users or user groups that should be exempt from the security checks of this exception rule. Enter the respective users or groups in the *Users/Groups* dialog box that opens after selecting the checkbox. Also, in Standard mode, matching for certain Users/Groups does not work due to the missing authentication.

Comment (optional): Add a description or other information about the exception.

3. Click **Save**.

The new exception appears on the *Exceptions* list.

To either edit or delete an exception list, click the corresponding buttons.

Advanced

The *Web Security >> HTTP/S >> Advanced* tab contains various other configuration options of the HTTP/S proxy such as caching or port settings.

Streaming settings:

Bypass content scanning for streaming content

When this option is active, typical audio and video streaming content is not subject to content scanning. Disabling this option will effectively disable most media streams, since they cannot be scanned in a reasonable timeframe. It is therefore recommended to leave this option turned on.

Transparent mode skip list:

Skip transparent mode hosts/nets

DND DND DND DND
DND DND DND DND
DND DND DND DND

Allow HTTP traffic for listed hosts/nets

IPs, URLs and Networks listed here will not be subject to the transparent interception of HTTP traffic. This affects both Sources and Destinations. If you want to allow unproxied HTTP traffic for the listed hosts or networks, make sure that the appropriate checkbox is checked.

Proxy Auto Configuration:

The proxy auto configuration is a feature that enables you to centrally provide a proxy auto configuration file (PAC file) which can be fetched by browsers. The browsers will in turn configure their proxy settings according to the details outlined in the PAC file. Use the text box below to enter the browser proxy configuration (in JavaScript) that should be delivered to the client with the PAC file.

Enable Proxy Auto Configuration

```
function FindProxyForURL(url, host)
{ return "PROXY proxy.example.com:8080; DIRECT"; }
```

Figure 10.6 Advanced HTTP/S Settings Part 1

Streaming Settings

Bypass Content Scanning for Streaming Content: When this option is active, typical audio and video streaming content is not subject to content scanning. Disabling this option will effectively disable most media streams, since they cannot be scanned in a reasonable timeframe. It is therefore recommended to leave this option turned on.

Transparent Mode Skip List

Using this option is only meaningful if the HTTP proxy runs in transparent mode. Hosts and networks listed in the *Skip Transparent Mode Hosts/Nets* box will not be subject to the transparent interception of HTTP traffic. This affects both source and destination hosts/networks. However, to allow HTTP

traffic (without proxy) for these hosts and networks, select the *Allow HTTP Traffic for Listed Hosts/Nets* checkbox. If you do not select this checkbox, you must define specific packet filter rules for the hosts and networks listed here.

Proxy Auto Configuration

The proxy auto configuration is a feature that enables you to centrally provide a proxy auto configuration file (PAC file) which can be fetched by browsers. The browsers will in turn configure their proxy settings according to the details outlined in the PAC file.

The PAC file is named *wpad.dat*, has the MIME type *application/x-nsp proxy-autoconfig* and will be provided by the ASG. It contains the information you enter into the text box, for example:

```
function FindProxyForURL(url, host)
{ return "PROXY proxy.example.com:8080; DIRECT"; }
```

The function above instructs the browser to redirect all page requests to the proxy of the server *proxy.example.com* on port 8080. If the proxy is not reachable, a direct connection to the Internet will be established.

To provide the PAC file for your network, you have the following possibilities:

- Providing via browser configuration: If you select the option *Enable Proxy Auto Configuration*, the PAC file will be available via the ASG HTTP proxy under the URL of the following type: *http://IP-of-ASG:8080/wpad.dat*. To use this file, enter its URL in the automatic proxy configuration setting of those browsers which are to use the proxy.
- Providing via DHCP: You can have your DHCP server(s) hand out the URL of the PAC file together with the client IP address. To do that, select the option *Enable HTTP Proxy Auto Configuration* in your DHCP server configuration (see chapter *Network Services >> DHCP*). A browser will then automatically fetch the PAC file and configure its settings accordingly.

Note – Providing via DHCP works with Microsoft's Internet Explorer only. Regarding all other browsers you need to provide the PAC file manually.

Misc Settings

HTTP Proxy Port: Here can you define the port number that the http proxy will use for client requests. The default is 8080.

Note – This only applies if you do not operate the proxy in transparent mode.

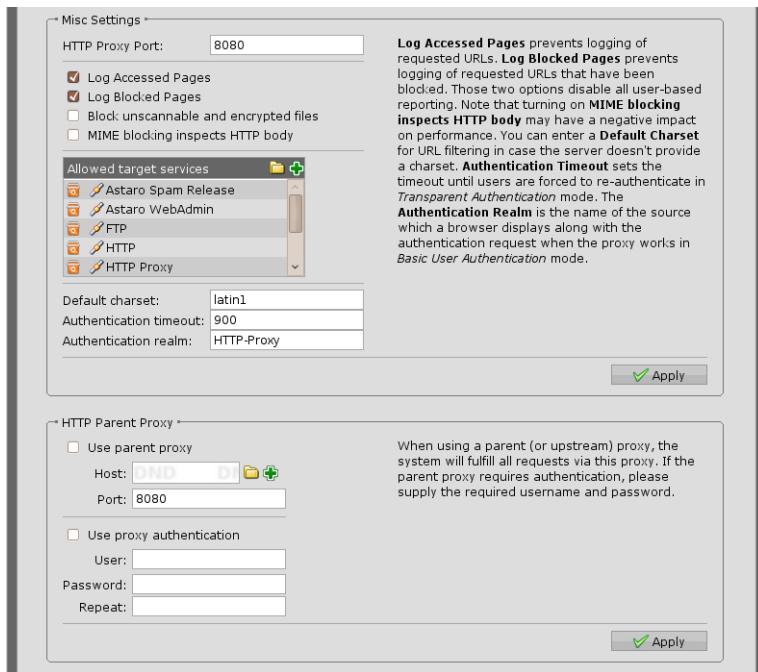


Figure 10.7 Advanced HTTP Settings Part 2

Log Accessed Pages: Select to log accessed URLs along with username and client IP of the request.

Log Blocked Pages: Select to log blocked URLs along with username and client IP of the request.

Note – The log options can be also set individually by means of an exception (see section *Exceptions*) or a filter action for profiles (see chapter *Web Security >> HTTP/S Profiles >> Filter Actions*).

Block Unscannable and Encrypted Files: Select this option to block files that could not be scanned. The reason for that may be, among other things, that files are encrypted or corrupt.

MIME Blocking Inspects HTTP Body: HTTP traffic is checked for blocked MIME types. Note that turning on this feature may have a negative impact on performance.

Allowed Target Services: In the *Allowed Target Services* box you can select

the target services the HTTP proxy should be allowed to access. The default setting consists of target services (ports) that are usually safe to connect to and which are typically used by browsers, namely *HTTP* (port 80), *HTTPS* (port 443), *FTP* (port 21), *LDAP* (port 389), *LDAP-SSL* (port 636), *HTTP Proxy* (port 8080), *Astero Spam Release* (ports 3840-4840), and *Astero WebAdmin* (port 4444).

Default Charset: This option affects how the proxy displays filenames in the *Download Manager* window. URLs (and filenames that they may reference) that are encoded in foreign charsets will be converted to UTF-8 from the charset specified here unless the server sends a different charset. If you are in a country or region that uses a double-byte charset, you should set this option to the "native" charset for that country or region.

Authentication Timeout: This option allows you to set the number of minutes between user authentication prompts when using the transparent user authentication feature.

Authentication Realm: The authentication realm is the name of the source which a browser displays along with the authentication request when the proxy works in *Basic User Authentication* mode. It defines the protection space according to RFC 2617²⁶. You can give any string here.

HTTP Parent Proxy

A parent proxy is often required in those countries that require Internet access to be routed through a government-approved proxy server. If your security policy requires the use of a parent proxy, you can set it up here by selecting the host definition and port.

Use a Parent Proxy: Select the checkbox to enable parent proxy use. Enter the hostname and the port of the proxy.

This Proxy Requires Authentication: If the parent proxy requires authentication, enter username and password here.

HTTP Caching

Enable Caching: When this option is enabled, the HTTP proxy keeps an on-disk object cache to speed up requests to frequently visited web pages.

Cache SSL Content: With this option enabled, SSL-encrypted data will be stored unencrypted on disk as well.

Cache Content that Contains Cookies: Cookies are often used for authentication purposes. With this option enabled, HTTP answers containing cookies will be cached as well. This may be critical, as users requesting the same page are likely to get the cached page, containing the cookie of another user.

²⁶ <http://www.faqs.org/rfcs/rfc2617.html>

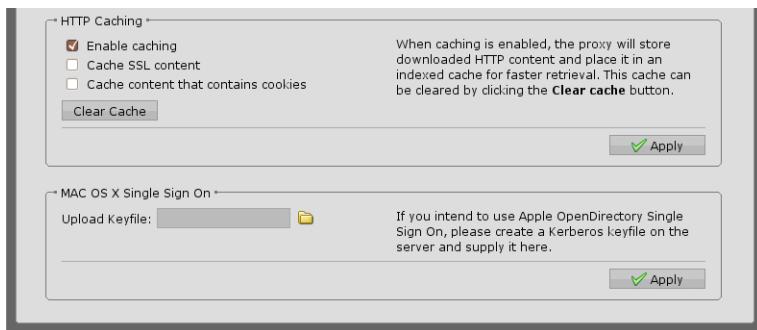


Figure 10.8 Advanced HTTP Settings Part 3

Important Note – Caching SSL and/or cookie content is an important security issue as the content is readable by every user with SuperAdmin rights.

Clear Cache: You can delete all cached pages by clicking *Clear Cache*.

MAC OS X Single Sign-On

When you are using *Apple OpenDirectory SSO* as authentication method, you need to upload a MAC OS X Single Sign-On Kerberos keyfile for authentication to work properly. Generate that keyfile and upload it by clicking *Upload Keyfile*. For more information on how to generate that keyfile please refer to the Kerberos documentation.

HTTPS CAs

On the *Web Security >> HTTP/S >> HTTPS CAs* tab you can manage Signing and Verification Certificate Authorities (CAs) for HTTPS connections.

Signing CA

In this area you can upload your Signing CA certificate, regenerate the Signing CA certificate, or download the existing Signing CA certificate. By default, the Signing CA certificate is created according to the information provided during setup, i.e. it is consistent with the information on the *Management >> System Settings >> Organizational* tab—unless there have been any changes applied since.

To upload a new Signing CA certificate, proceed as follows:

- 1. Click the button *Upload*.**

The *Upload PKCS#12 Certificate File* dialog box opens.

- 2. Browse for the certificate to upload.**

Click the folder icon next to the *File* box, click *Browse* in the opening *Upload File* dialog box, select the certificate to upload and click *Save*.

You can only upload certificates in PKCS#12 format which are password protected.

- 3. Enter the password.**

Enter the password twice into the corresponding fields and click *Save*.

The new Signing CA certificate will be installed.

To regenerate your Signing CA certificate, proceed as follows:

- 1. Click the button *Regenerate*.**

The *Create New Signing CA* dialog box opens.

- 2. Change the information.**

Change the given information according to your needs and click *Save*.

The new Signing CA certificate will be generated. The Signing CA information in the *Signing CA* area will change accordingly.

To download the Signing CA certificate, proceed as follows:

- 1. Click the button *Download*.**

The *Download Certificate File* dialog box opens.

- 2. Select the file format to download.**

You can choose between two different formats:

- **PKCS#12:** This format will be encrypted, so enter an export password.
- **PEM:** Unencrypted format.

- 3. Click *Save*.**

Click *Save* to save the file.

If you use certificates for your internal webservers signed by a custom CA, it is advisable to upload this CA certificate to WebAdmin as Trusted Certificate Authority. Otherwise users will be prompted with an error message by the HTTP proxy claiming to be confronted with an untrustworthy server certificate.

To facilitate supplying client PCs with the proxy CA certificate, users can download the certificate themselves via <http://passthrough.fw-notify.net/cacert.pem> and install it in their browser. The website request is directly accepted

and processed by the proxy. It is therefore necessary to enable the HTTPS proxy on the *Web Security >> Global* tab first.

Note – In case the proxy's operation mode is not *Transparent Mode* the proxy has to be enabled in the user's browser. Otherwise the certificate download link will not be accessible.

Alternatively, if the User Portal is enabled, users can download the proxy CA certificate from the User Portal, tab *HTTPS Proxy*.

Preventing HTTPS Problems

When using HTTPS, Windows system programs like Windows Update and Windows Defender will not be able to establish connections because they are run with **system** user rights. However, this user, by default, does not trust the proxy CA. It is therefore necessary to import the HTTPS proxy CA certificate for the system user. Do the following:

1. In Windows, open the *Microsoft Management Console (mmc)*.
2. Click on the *File* menu and then *Add/Remove Snap-in*.
The *Add or Remove Snap-ins* dialog window opens.
3. Click **Add** at the bottom of the window.
The dialog window *Add Standalone Snap-In* opens.
4. Select *Certificates* from the list and click **Add**.
A wizard appears.
5. Select *Computer account* and click **Next**.
6. Make sure that *Local computer* is selected and click **Finish** and then **Close**.
The first dialog window now contains the item *Certificates (Local Computer)*.
7. Click **OK**.
The dialog window closes and the *Console Root* now contains the item *Certificates (Local Computer)*.
8. In the *Console Root* window on the left open *Certificates >> Trusted Root Certification Authorities*, right-click *Certificates* and select *All Tasks >> Import* from the context menu.
The import dialog wizard opens.

9. Click Next.

The next wizard step is displayed.

10. Browse to the previously downloaded HTTPS proxy CA certificate, click Open and then Next.

The next wizard step is displayed.

11. Make sure that Place all certificates in the following store is selected and click Next and Close.

The wizard reports the import success.

12. Confirm the wizard's message.

The Proxy CA certificate is now displayed among the trusted certificates.

13. Save the changes.

Click on the *File* menu and then *Save* to save the changes on the Console Root.

After importing, the CA is system-wide accepted and connection problems resulting from the HTTPS proxy should not occur.

Verification CAs

This area allows you to manage Verification CAs. Those are Certificate Authorities you trust in the first place, i.e. websites presenting valid certificates signed by these CAs are regarded trustworthy by the HTTPS proxy.

Local Verification CAs: You can upload Verification CAs additionally to the CA list below. Proceed as follows:

1. Click the folder icon next to the *Upload Local CA* field.

The *Upload File* dialog box opens.

2. Select the certificate to upload.

Click *Browse* and select the CA certificate to upload.

3. Upload the certificate.

Click *Start Upload* to upload the selected CA certificate.

The certificate will be installed and displayed in the *Local Verification CAs* area.

Global Verification CAs: The list of Verification CAs shown here is identical to the Verification CAs pre-installed by Mozilla Firefox. However, you can disable one or all Verification CAs of the list if you do not regard them as trustworthy. To revoke a CA's certificate click its status icon. The status icon turns red and the HTTPS proxy will no longer accept websites signed by this CA.

Tip – Click the blue information icon to see the fingerprint of a CA.

The HTTPS proxy will present a "Blocked Content" error page to a client if the CA is unknown or disabled. However, you can create an exception for such pages: either via the *Create Exception* link on the error page of the proxy or via the *Web Security >> HTTP/S >> Exceptions* tab.

Note – When clicking the *Create Exception* link on the proxy error page a login dialog window is presented. Only users with admin rights are allowed to create exceptions.

HTTP/S Profiles

Astaro Security Gateway features an HTTP/S proxy designed and optimized for controlling what web content is available on a particular network. It thus prevents persons from viewing content which you may consider objectionable. You can configure the HTTP/S proxy to apply globally to selected networks. Alternatively, you can create individual proxy profiles that can be used to enforce various security policies to be applied to different segments of your network. That way you can define different content filtering policies for the various departments within your organization, even with varying user authentication methods.

Cross Reference – More information on how to configure HTTP/S profiles can be found in the Astaro knowledgebase²⁷ (navigate to *ASG Version 7 >> Web Security*).

This chapter describes how to add filter actions and how to use them in the HTTP/S profiles framework of Astaro Security Gateway. You are advised to configure the *HTTP/S Profiles* tabs from backward to forward. That is to say, begin with specifying your filter actions first, which are then assigned to particular users and user groups in so-called filter assignments, which in turn are taken to configure the actual proxy profiles.

²⁷ <http://www.astaro.com/kb/>

Overview

Note – To configure HTTP profiles, the HTTP proxy must be enabled.

The flowchart shows how filter actions, filter assignments, and proxy profiles interact. If an HTTP request comes in, the HTTP proxy first determines which proxy profile must be applied. This is entirely dependent on the source IP address of the request. The first profile that matches the source IP of the request will be used. All other proxy profiles that may exist will be ignored.

Internally, all profiles are stored in a single file with the default profile being at the bottom of the list. In the beginning, when no other HTTP profile is configured, the default profile is the only one present. When you start adding individual proxy profiles and sort them using the *Position* drop-down list, the default profile will stay at the end of list, thus making sure that it will always be applied last.

The default profile, however, is *not* a profile to be explicitly configured on the *Web Security >> HTTP/S Profiles* tabs. Instead, it is automatically created when you globally configure the HTTP proxy on the *Web Security >> HTTP/S* tabs. The *Allowed Networks* to be configured on the *Web Security >> HTTP/S >> Global* tab correspond to the *Source Networks* of a proxy profile. The settings in the *Users/Groups* box (located on *Web Security >> HTTP/S >> Global* tab when operation mode *Basic User Authentication* is selected) become the default filter assignment, while the settings on the *Web Security >> HTTP/S >> URL Filtering* tab correspond to a filter action. Finally, if not even the default profile matches, the HTTP request will be blocked.

It is then checked which filter assignment is associated with this proxy profile. If no filter assignment matches, the fallback action will be applied to the request. The fallback action is a special filter action that should reflect the security policy of your company. If you must adhere to a strict security policy, you could create a filter action that blocks all web traffic without exception.

To provide different levels of protection for various users within the same network segment, you only need to configure one single proxy profile with different filter assignments associated. What is allowed for specific users is dependent upon the order of the selected filter assignments. For that reason it does not make sense to configure two profiles with exactly the same source networks, as the second profile will never be used.

Proxy Profiles

Proxy profiles can be used to create various content filtering policies, enabling you to apply different policies to different addresses of your network. That way you can define different policies for the various departments within your organization. In addition, each proxy profile can have its own user authentication method.

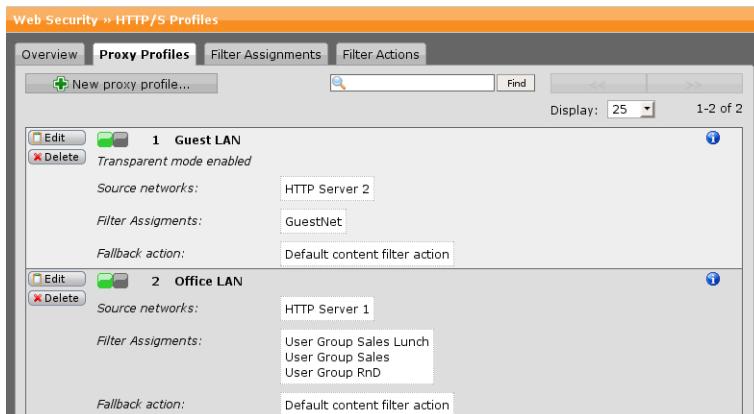


Figure 10.9 Proxy Profile List

To create a proxy profile, proceed as follows:

1. **Click New Proxy Profile.**

The *Create Proxy Profile* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for this profile.

Position: The position number, defining the priority of the proxy profile. Lower numbers have higher priority. Proxy profiles are matched in ascending order. Once a proxy profile has matched, proxy profiles with a higher number will not be evaluated anymore. Place the more specific profiles at the top of the list to make sure that less restrictive profiles match last.

Source Networks: Select the networks that should use this proxy profile (note that this field is mandatory).

Caution – Make sure to not select source networks here that are used in other proxy profiles because this may lead to an inconsistent mapping between content filter actions and users/groups, possibly allowing users who

reside in a certain network segment to open websites you do not want them to access.

Filter Assignments: Select a filter assignment. A filter assignment is a set of web security configuration settings that can be used to assign different levels of protection to various users/groups at various times (for more information, see *Web Security >> HTTP/S Profiles >> Filter Assignments*). Note that you can select multiple filter assignments. In addition, you can specify which filter assignment should be applied first. This is useful, for example, if you want to assign different filter assignments for the same users or user groups to be applied at different times. Generally speaking, place the more specific assignments at the top of the list to make sure that the least restrictive assignments match last. For this, use the blue arrows that appear after you have selected at least two filters.

Note – You can also select a *Default Filter Assignment*, which has assigned the *Default Filter Action* to the users/groups configured on the *HTTP/S >> Global* tab, provided the HTTP/S proxy runs in either *Basic User Authentication*, *Active Directory SSO*, or *eDirectory SSO* mode. Note further that you can use a filter assignment that has users and groups selected even when you set the operation mode to *standard* or *transparent*, but in that case, the users and groups will be ignored and only the time events specified in the filter assignment will be taken into account when using this proxy profile.

Fallback Action: The fallback action is a special filter action that should reflect the security policy of your company and will be applied to the request if none of the selected filter assignments matches. For example, if you must adhere to a strict security policy, you could create a special filter action as fallback that blocks all web traffic without exception. In addition, the *Default Filter Action* you can select here corresponds to the settings of the *Web Security >> HTTP/S >> URL Filtering* tab.

Operation Mode: For each proxy profile, you can select among several user authentication methods. Different proxy profiles can have different authentication methods, but only one user authentication method can be used for each proxy profile. You can even select a different operation mode than configured on the *HTTP/S >> Global* tab. Note, however, that authentication will only work as expected if the authentication mode selected here

matches the authentication mode of all user and group objects used in all filter assignments. The following modes are available:

- **Standard:** In standard mode, the HTTP proxy will listen for client requests on port 8080 by default and will allow any client from the networks listed in *Allowed Networks* box to connect. When used in this mode, clients must have specified the HTTP proxy in their browser configuration.
- **Active Directory SSO:** Select when you have configured *Active Directory Single Sign-On* (SSO) on the *Users >> Authentication >> Servers* tab. This has the effect that NTLM user authentication will be used to authenticate clients. Note that this is only guaranteed to work with Internet Explorer. When used in this mode, clients must have specified the HTTP proxy in their browser configuration.
- **Apple OpenDirectory SSO:** Select when you have configured *LDAP* on the *Users >> Authentication >> Servers* tab and you are using Apple OpenDirectory. Additionally, you have to upload a MAC OS X Single Sign-On Kerberos keyfile on the *Web Security >> HTTP/S >> Advanced* tab for the proxy to work properly. When the HTTP proxy is used in this mode, clients must have specified the HTTP proxy in their browser configuration. Note that the Safari browser does not support SSO.
- **Basic User Authentication:** In *Basic User Authentication* mode, each client must authenticate itself against the proxy before using it. For more information about which authentication methods are supported, see *Users >> Authentication*. When used in this mode, clients must have specified the HTTP proxy in their browser configuration.
- **eDirectory SSO:** Select when you have configured *eDirectory* on the *Users >> Authentication >> Servers* tab. When used in this mode, clients must have specified the HTTP proxy in their browser configuration.
- **Transparent:** In transparent mode, all connections made by client browser applications on port 80 (port 443, respectively, if SSL is used) are intercepted and redirected to the proxy without client-side configuration. The client is entirely unaware of the proxy server. The advantage of this mode is that no additional administration or client-side configuration is necessary, the disadvantage however is that only HTTP (port 80) requests can be processed. Thus, when you select *Transparent* as

mode, the client's proxy settings will become ineffective.

Full Transparent Mode (optional): Select the checkbox *Full Transparent Mode* to preserve the client source IP instead of replacing it by the firewall's IP. This is useful if your clients use public IP addresses that should not be disguised by the proxy.

Note – In transparent mode, the proxy will strip NTLM authentication headers from HTTP requests. Furthermore, the proxy cannot handle FTP requests in this mode. If your clients want to access such services, you must open the port (21) in the packet filter. Note further that some web servers transmit some data, in particular streaming video and audio, over a port different from port 80. These requests will not be noticed when the proxy operates in transparent mode. To support such traffic, you must either use a different mode or enter an explicit packet filter rule allowing them.

- **Transparent with Authentication:** Use this mode to force users to authenticate while the proxy is working transparently. When users open a website for the first time, they will be presented an authentication user-portal-like webpage where they have to fill in username and password. This mode allows for username-based tracking, reporting, and surfing without client-side browser configuration. Moreover, you can enable a disclaimer that is additionally displayed on that dialog window and needs to be accepted by users to be able to go on. For more information on the disclaimer, please refer to chapter *Management >> Customization >> HTTP/S Proxy*.

Scan HTTPS (SSL) Traffic: Select the checkbox to not only scan HTTP traffic but HTTPS traffic, too.

Comment (optional): Add a description or other information about the proxy profile.

3. Click **Save**.

The new profile appears on the *Proxy Profiles* list.

To either edit or delete a proxy profile, click the corresponding buttons.

Filter Assignments

On the *HTTP/S Profiles >> Filter Assignment* tab you can assign filter actions to particular users and user groups. While a filter action rather refers to the

"What" by defining which websites or categories of websites should be blocked, a filter assignment refers to the "Who" and "When" by assigning those actions to users and user groups at specific times.

Note – Various settings you have configured on the *Web Security >> HTTP/S >> AntiVirus/Malware* tab (AntiVirus scanning, file extension filter, MIME type filter, content removal) and the *URL Filtering* tab (categories, blocked URLs) are stored as a *Default Filter Action*, which can be selected from the *Filter Action* drop-down list below.

User/Groups	Filter Action	Time Event
RnD	Allow All	Always
Sales	Microsoft Update	Always
Sales	Moderate	Lunch

Figure 10.10 Filter Assignments List

To create a filter assignment, proceed as follows:

1. **Click *New Filter Assignment*.**

The *Create New Filter Assignment* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for this assignment.

Users/Groups: Select the users and groups that should use a specific filter action. Note that your new filter assignment should only be added to proxy profiles using the same authentication mode as the users and groups you select here.

Time Event: Time events are single or recurring time slots that can be used to limit packet filter rules or filter profiles to specific time ranges. For more information, see *Definitions >> Time Events*.

Filter Action: Select the filter action you want to assign to the users and

user groups defined above.

Comment (optional): Add a description or other information about the content filter profile.

3. Click Save.

The new assignment appears on the *Filter Assignments* list.

To either edit or delete a filter assignment, click the corresponding buttons.

Each filter assignment can be selected when creating a proxy profile.

Filter Actions

On the *HTTP/S Profiles >> Filter Actions* tab you can create and edit a set of web security configuration settings that can be used to customize different types and levels of protection. Filter actions can be assigned to different users and user groups, providing a flexible way to control web access.

The screenshot shows the 'Filter Actions' tab of the 'HTTP/S Profiles' section. The interface includes a toolbar with 'New filter action', search, and display controls. Below is a table listing five filter actions:

Action	Mode	Setting
Allow All	Blacklist	Spyware is blocked
Default content filter block action	Whitelist	Anti-Virus scanning Dual Scan
Microsoft Update	Whitelist	Allowed Sites microsoft.com
Moderate	Blacklist	Content removal JavaScript Embedded
		Anti-Virus scanning Single Scan
		Blocked SP Categories Extremistic Sites, Nudity, Weapons, Drugs, Job Search, Criminal Activities
		Spyware is blocked
		Anti-Virus scanning Dual Scan

Figure 10.11 Filter Actions List

To create a filter action, proceed as follows:

1. Click New Filter Action.

The *Create New Filter Action* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for this action.

Mode: Select whether your selection of websites should be blocked or allowed. The following options are available:

- **Allow By Default:** If this option is selected, your selection of websites will be blocked while all other websites will be allowed.
- **Block By Default:** If this option is selected, all websites except the ones you selected will be blocked.

Threshold: Websites can be classified as either *Trusted*, *Neutral*, or *Suspicious*. Unclassified websites are referred to as *Unverified*. You can determine which reputation a website must have to be accessible from your network. Websites below the selected threshold will be blocked.

Block Spyware Communication: Selecting this option will detect and block spyware on the way from the server to the client. This prevents computers within your network from getting infected by new spyware. Moreover, activating this feature will detect and block traffic from already installed spyware applications. That way, gathered user information will no longer be submitted to the Internet. Note that this option is not available if you change the mode to *Block By Default*.

Block these Website Categories: Select the website categories that should be blocked. Note that this option is changed to *Allow these Website Categories* if *Mode* is set to *Block by Default* above.

Block Uncategorized Sites: Enabling this option will prevent the browser from opening websites of unknown content. This function can be considered as a fallback security mechanism in case a potentially unwanted website has not yet been categorized as such. Note that this option is changed to *Allow Uncategorized Sites* if *Mode* is set to *Block by Default* above.

Block these URLs/Sites: Enter the URL of sites to be blocked.

Always Allow these URLs/Sites: Enter the URL of sites to be always allowed.

Blocked File Extensions: By specifying a file extension, you can block certain types of files based on their extensions (e.g., executable binaries). To add a file extension, click the plus icon in the *Blocked File Extensions* box and enter the extension you want to block, for example `exe` (without the delimiting dot).

Blocked MIME Types: To add a MIME type that shall be blocked, click the plus icon in the *Blocked MIME Types* box and enter the MIME type (e.g.,

image/gif).

Content Removal: When selected, the *Remove JavaScript* and *Remove Embedded* options become visible. Using these options you can configure whether <SCRIPT> and <OBJECT> tags shall be removed from HTML pages, on the one hand deactivating JavaScript functions that are embedded in or included from HTML pages, on the other hand stripping off dynamic content such as ActiveX, Flash or Java applets from the incoming HTTP/S traffic.

Use AntiVirus Scanning: When selecting this option, inbound web traffic is scanned for malicious content. Astaro Security Gateway features several antivirus engines for best security.

Max Scanning Size: Specify the maximum size of files to be scanned by the antivirus engine(s). Files exceeding this size will be exempt from scanning. The following two options are useful if there are persons or members of e.g. a works council whose activities must not be logged at all:

Log Accessed Pages: Unselect to exclude accessed pages from logging and reporting.

Log Blocked Pages: Unselect to exclude blocked pages from logging and reporting.

3. Click Save.

The new filter action appears on the *Filter Actions* list.

To either edit or delete a filter action, click the corresponding buttons.

Each filter action can be selected when creating a filter assignment or proxy profile.

Note – You can see here also the *Default Content Filter Block Action* which by default blocks every HTTP/S request that does not match any other filter action or the settings in the *HTTP/S* menu.

FTP

On the *Web Security >> FTP* tab you can configure the FTP proxy. The *File Transfer Protocol* (FTP) is a widely used protocol for exchanging files over the Internet. Astaro Security Gateway presents a proxy service acting as a go-between for all FTP traffic passing your network. The FTP proxy provides such useful features as virus scanning of FTP traffic or blocking of certain file types that are transferred via the FTP protocol.

The FTP proxy can work transparently, that is, all FTP clients within your network would establish a connection to the proxy instead of their ultimate destination. The proxy would then initiate a new network connection on behalf of the request, invisible to the client. The advantage of this behavior is that no additional administration or configuration on client-side is necessary.

Global

On the *Web Security >> FTP >> Global* tab you can configure the basic settings of the FTP proxy.

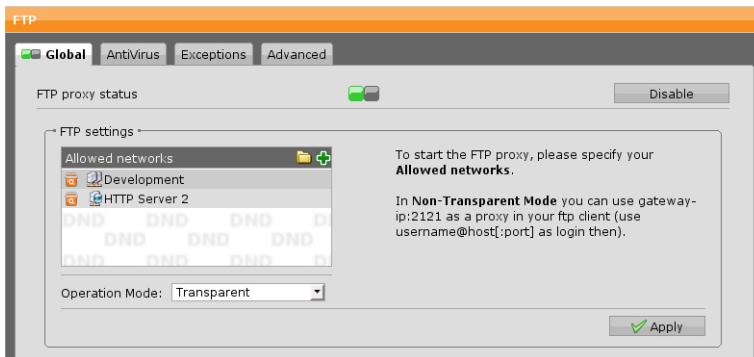


Figure 10.12 Configuring the FTP Proxy

To configure the FTP proxy, proceed as follows:

1. On the *Global* tab, enable the FTP proxy.

You can either click the status icon or the *Enable* button.

The status icon turns amber and the Global FTP Settings area becomes editable.

2. Select the *Allowed Networks*.

Select the networks that are allowed to use the FTP proxy.

3. Select an operation mode.

Select an operation mode for the FTP proxy. The following modes are available:

- **Transparent:** The proxy forwards the client request to the target server and scans the content. No configuration on client side is necessary.
- **Non-Transparent:** Using this mode you need to configure the FTP clients. Use the firewall's IP address and port 2121.
- **Both:** This mode allows you to use transparent mode for some clients and non-transparent mode for others. Configure FTP clients that are to work in non-transparent mode to use a proxy with the firewall's IP address and port 2121.

4. Click **Apply**.

Your settings will be saved.

Note – The FTP proxy is unable to communicate with FTP servers that use Active Directory authentication. To enable FTP clients to connect to an FTP server of that kind, add the server to the FTP proxy skip list, which is configured on the *Web Security >> FTP >> Advanced* tab.

AntiVirus

The *Web Security >> FTP >> AntiVirus* tab contains all measures that can be taken against FTP traffic that carries harmful and dangerous content such as viruses, worms, or other malware.

Use AntiVirus Scanning: When selecting this option, the entire FTP traffic will be scanned. Astaro Security Gateway features several antivirus engines for best security.

- **Single Scan:** Default setting; provides maximum performance.
- **Dual Scan:** Provides maximum recognition rate by scanning all FTP traffic twice using different virus scanners.

Max Scanning Size: Specify the maximum size of files to be scanned by the antivirus engine(s). Files exceeding this size will be exempt from scanning. Click **Apply** to save your settings.

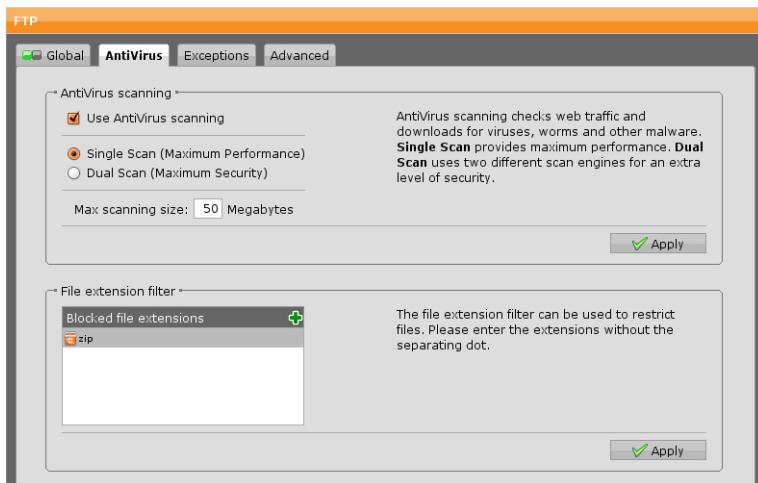


Figure 10.13 Configuring FTP Proxy AntiVirus Settings

File Extension Filter

This feature filters FTP transfers that transmit certain types of files based on their extensions (e.g., executable binaries) from web traffic that have a file extension listed in the *Blocked File Extensions* box. You can add additional file extensions or delete file extensions that are not to be blocked. To add a file extension, click the plus icon in the *Blocked File Extensions* box and enter the file extension you want to block, for example `exe` (without the delimiting dot). Click *Apply* to save your settings.

Note – Encrypted zip archives cannot be scanned for malicious content and will pass through the virus scanner. To protect your network from malware included in encrypted zip files you might want to consider blocking the zip file extension altogether.

Exceptions

On the *FTP >> Exceptions* tab you can define whitelist hosts/networks that should be excluded from selectable security options offered by the FTP proxy.

To create an exception, proceed as follows:

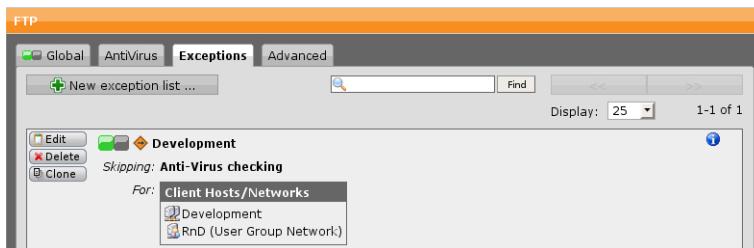


Figure 10.14 FTP Proxy Exceptions List

1. On the **Exceptions** tab, click *New Exception List*.

The *Create Exception List* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for this exception.

Skip These Checks: Select the security checks that should be skipped:

- **AntiVirus Checking:** Select to disable virus scanning, which checks traffic for unwanted content such as viruses, trojan horses, and the like.
- **Extension Blocking:** Select to disable the file extension filter, which can be used to block file transfers based on file extensions.
- **Allowed Servers:** Select to disable checks for allowed servers which can be set on the *Advanced* tab.

For These Client Hosts/Networks: When selecting this option, the *Client Hosts/Networks* box opens.

Select the client hosts/networks that should be exempt from the security checks of this exception rule.

For These Server Hosts/Networks: When selecting this option, the *Server Hosts/Networks* box opens.

Select the servers that should be exempt from the security checks of this exception rule.

Comment (optional): Add a description or other information about the exception.

3. Click **Save**.

The new exception list appears on the *Exceptions* list.

To either edit or delete an exception list, click the corresponding buttons.

Advanced

On the *FTP >> Advanced* tab you can specify hosts and networks that can skip the transparent mode of the FTP proxy.

Note – The FTP proxy is unable to communicate with FTP servers that use Active Directory authentication. To enable FTP clients to connect to an FTP server of that kind, add the server to the FTP proxy skip list.

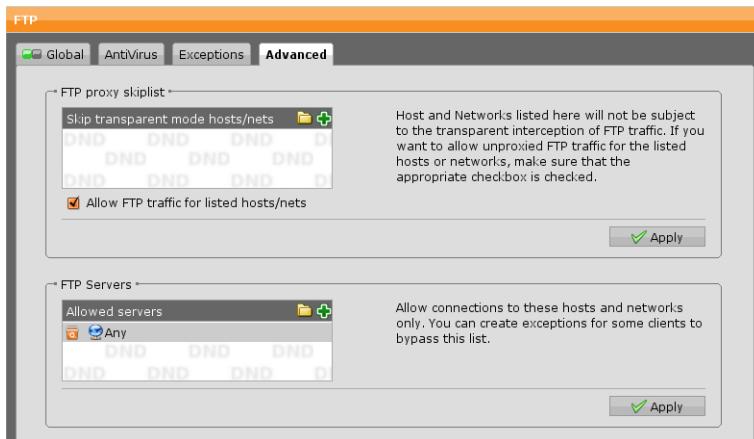


Figure 10.15 Configuring Advanced FTP Proxy Settings

FTP Proxy Skip list

Hosts and networks listed here are excluded from the transparent interception of FTP traffic. However, to allow FTP traffic for these hosts and networks, select the *Allow FTP Traffic* checkbox. If you do not select this checkbox, you must define specific packet filter rules for the hosts and networks listed here.

FTP Servers

Select or add FTP servers that are allowed to access from your network. You can create exceptions for some clients to bypass this list on the *Exceptions* tab.

Mail Security

This chapter describes how to configure basic e-mail security features of Astaro Security Gateway. The *Mail Security Statistics* page in WebAdmin shows an overview of today's top ten e-mail senders, e-mail recipients, spammers (by country), recognized malware, and concurrent connections. Each of the sections contains a *Details* link. Clicking the link redirects you to the respective *Reporting* section of WebAdmin, where you can find more statistical information.

The following topics are included in this chapter:

- SMTP
- SMTP Profiles
- POP3
- Encryption
- Quarantine Report
- Mail Manager

SMTP

The menu *Mail Security >> SMTP* allows you to configure the SMTP proxy. SMTP is the abbreviation of *Simple Mail Transfer Protocol*, a protocol used to deliver e-mails to a mail server. Astaro Security Gateway includes an application level gateway for SMTP, which can be used to protect your internal mail server from remote attacks and additionally provides powerful virus scanning and e-mail filtering services.

Note – To use the SMTP proxy correctly, a valid name server (DNS) must be configured.

Global

On the *Mail Security >> SMTP >> Global* tab you can decide whether to use *Simple Mode* for SMTP configuration or *Profile Mode*.

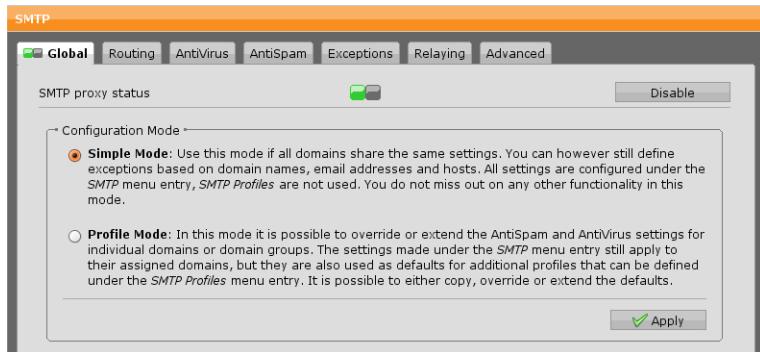


Figure 11.1 Enabling the SMTP Proxy

1. Enable SMTP.

You can either click the status icon or the *Enable* button. The status icon turns green and the Configuration Mode becomes editable.

2. Select a configuration mode.

Simple Mode: Use this mode if all domains share the same settings. However, you can still define exceptions based on domain name, e-mail addresses, and hosts. There is no functionality restriction compared with *Profile Mode*.

Profile Mode: In this mode you can override or extend global settings e.g., of antispam and antivirus, for individual domains or domain groups by creating profiles for them in the menu *SMTP Profiles*. Settings made in the *SMTP* menu still apply to their assigned domains and, moreover, serve as defaults for profiles. In *Profile Mode*, you will find additional notes with some of the settings regarding recommendations for profile mode and behavior of the ASG.

3. Click *Apply*.

The selected mode will be enabled.

Routing

On the *Routing* tab you can configure domain and routing targets for the SMTP proxy and define how recipients are to be verified.

To configure the SMTP proxy routing, proceed as follows:

1. Enter your internal domain(s).

To enter your e-mail domains, click the plus icon in the *Domains* box.

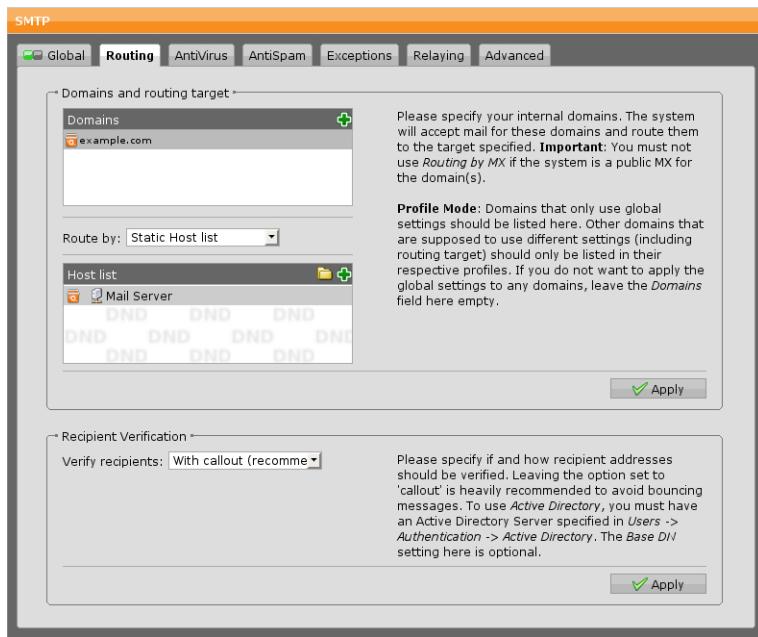


Figure 11.2 Configuring Domains and Routing Targets

In the appearing text box, enter the domain in the form `example.com` and click *Apply*. Repeat this step until all domains are listed.

In Profile Mode: Enter only domains that use global settings. All other domains should be listed in their respective profiles.

2. Specify the internal server.

From the drop-down list *Route By*, select the host to which e-mails for the domains listed above should be forwarded to. A typical target host would be the Microsoft Exchange Server on your local network. You can choose between different server types:

- **Static Host List:** Select a host definition of the target route in the *Host List* box. Note that you can select several host definitions for basic failover purposes. If delivery to the first host fails, mail will be routed to the next one. However, the (static) order of hosts cannot be determined with the current version of Astaro Security Gateway and is somewhat accidental. To randomize delivery to a group of hosts so as to additionally achieve basic load balancing capability, use the *DNS Hostname*

route type and specify a hostname that has multiple A records (an *A record* or *address record* maps a hostname to an IP address).

- **DNS Hostname:** Specify the *fully qualified domain name* (FQDN) of your target route (e.g., `exchange.example.com`). Note that when you select a DNS name having multiple A records, mail to each server will be delivered randomly. In addition, if one server fails, all mail destined for it will automatically be routed to the remaining servers.
- **MX Records:** You can also route mail to your domain(s) by means of MX record(s). When this route type is selected, the mail transfer agent of Astaro Security Gateway makes a DNS query requesting the MX record for the recipient's domain name, which is the portion of the e-mail address following the "@" character. If you select this route type, make sure that the firewall is not the primary MX for the domain(s) specified above, since it will not deliver mail to itself.

3. Click **Apply**.

Your settings will be saved.

Recipient verification

Verify recipients: Here you can specify whether and how e-mail recipients are to be verified.

- **With Callout:** A request is sent to the server to verify the recipient.
- **In Active Directory:** A request is sent to the Active Directory server to verify the recipient. To be able to use Active Directory you must have an Active Directory server specified in *Users >> Authentication >> Servers*. Enter a Base DN into the *Alternative Base DN* field.

Note – The use of Active Directory recipient verification may lead to bounced messages in case the server does not respond.

- **Off:** You can turn off recipient verification completely but this is not recommended for it will lead to higher spam traffic volume and dictionary attacks. Thus your quarantine is likely to be flooded with unsolicited messages.

Click *Apply* to save your settings.

AntiVirus

The *AntiVirus* tab contains various measures against e-mails that carry harmful and dangerous content such as viruses, worms, or other malware.

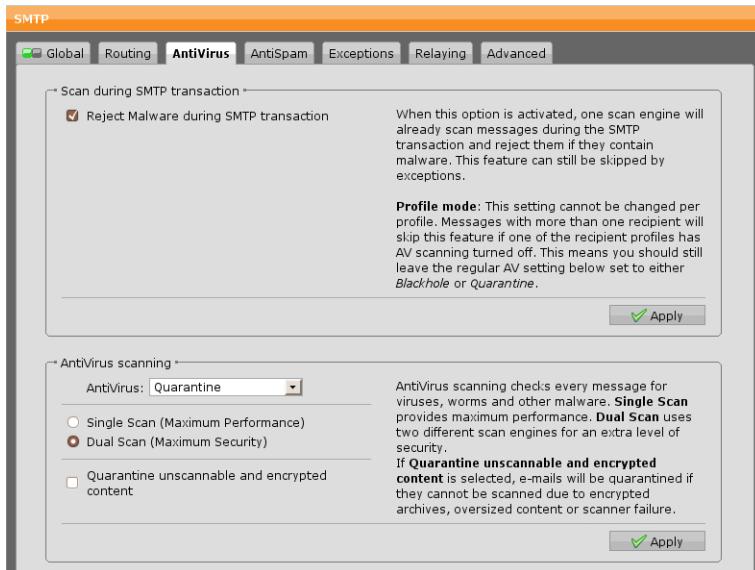


Figure 11.3 Configuring AntiVirus Settings of the SMTP Proxy

Scan During SMTP Transaction

Select the checkbox *Reject Malware During SMTP Transaction* if you want to have messages scanned already during SMTP transaction and to have them rejected in case they contain malware.

In Profile Mode: This setting cannot be changed per profile. Messages with more than one recipient will skip this feature if one of the recipient profiles has *AntiVirus Scanning* turned off. This means it is advisable to leave the regular antivirus setting below set to either *Blackhole* or *Quarantine*.

AntiVirus Scanning

When using this option, e-mails will be scanned for unwanted content such as viruses, trojan horses, or suspicious file types. Messages containing malicious content will be blocked and stored in the e-mail quarantine. Users can review and release their quarantined messages either through the Astaro User Portal or the daily Quarantine Report. However, messages containing malicious content can only be released from the quarantine by the administrator in the Mail Manager.

AntiVirus: You can configure how to proceed with messages that contain malicious content. The following actions are available:

- **Off:** There will be no antivirus scans.
- **Blackhole:** The message will be accepted and instantly removed.
- **Quarantine:** The message will be blocked and stored in the e-mail quarantine. Quarantined messages can be reviewed either through the User Portal or the daily Quarantine Report. Note that messages containing malicious content can only be released from the quarantine by an administrator.

Astaro Security Gateway features several antivirus engines for best security.

- **Single Scan:** Default setting; provides maximum performance.
- **Dual Scan:** Provides maximum recognition rate by scanning all e-mails twice using different virus scanners.

Quarantine Unscannable and Encrypted Content: When you select this option, e-mails with content that cannot be scanned will be quarantined. Unscannable content may be encrypted or corrupt archives or oversized content, or there may be a technical reason like a scanner failure.

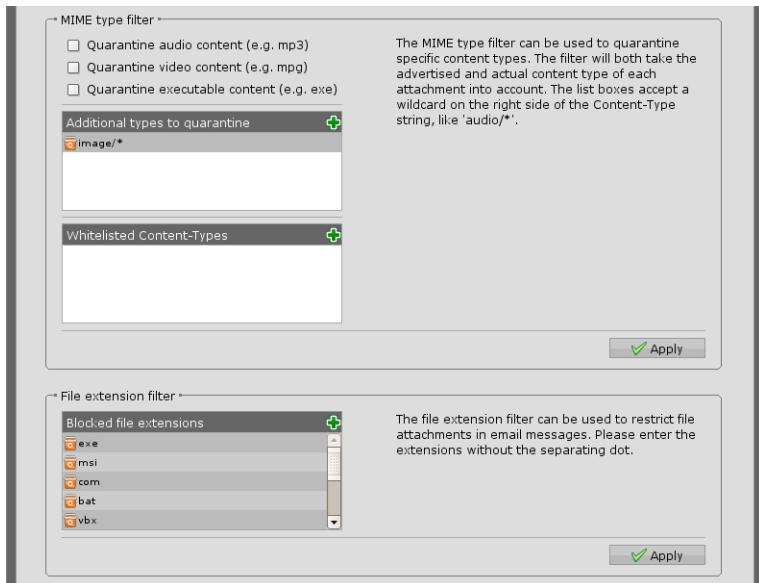


Figure 11.4 File Extension Filter on the AntiVirus Tab

MIME Type Filter

The MIME type filter reads the MIME type of e-mail contents. You can define how the different MIME types are to be dealt with.

- **Quarantine Audio Content:** When you select this checkbox audio content like e.g., mp3 or wav files, will be quarantined.
- **Quarantine Video Content:** When you select this checkbox video content like e.g., mpg or mov files, will be quarantined.
- **Quarantine Executable Content:** When you select this checkbox executable content like e.g., exe files, will be quarantined.

Additional Types To Quarantine: To add a MIME type other than above that shall be quarantined, click the plus icon in the *Additional Types To Quarantine* box and enter the MIME type (e.g., image/gif). You can use wildcards (*) on the right side of the slash, e.g., application/*.

Whitelisted Content-Types: You can use this box to allow generally certain MIME types. To add a MIME type click the plus icon in the *Whitelisted Content-Types* box and enter the MIME type.

MIME type	MIME type class
audio/*	audio files
video/*	video files
application/x-dosexec	applications
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 types known by the MIME Type Filter

File Extension Filter

Using the *File Extension Filter* you can quarantine e-mails (with warnings) that contain certain types of files based on their extensions (e.g., executables). To

add file extensions, click the plus icon in the *Blocked File Extensions* box and enter a critical file extension you want to be scanned, e.g., exe or jar (without the dot delimiter).

Note – Encrypted zip archives cannot be scanned for malicious content and will pass through the virus scanner. To protect your network from malware included in encrypted zip files you might want to consider blocking the zip file extension altogether.

AntiVirus Check Footer

For each outgoing e-mail, you can add and customize a special footer informing users that the e-mail has been scanned for malicious content. However, the antivirus check footer will not be appended to the e-mail if the e-mail is a reply (i.e. having *In-Reply-To* header) or if the content type of the e-mail could not be determined.

Note – Adding a footer to messages already signed or encrypted by an e-mail client (e.g., Microsoft's Outlook or Mozilla's Thunderbird) will break their signature and render them invalid. If you want to create digital signatures on the client side, disable the antivirus check footer option. However, if you do not wish to forgo the privacy and authentication of your e-mail communication and still want to apply a general antivirus check footer, consider using the built-in feature of Astaro Security Gateway. E-mail encryption done on the gateway means that the footer is added to the message prior to creating the digital signature, thus leaving the signature intact.



Figure 11.5 AntiVirus Check Footer on the AntiVirus Tab

AntiSpam

Astaro Security Gateway can be configured to detect unsolicited spam e-mails and to identify spam transmissions from known or suspected spam purveyors. Configuration options located on the *AntiSpam* tab let you configure SMTP security features aimed at preventing your network from receiving unsolicited commercial e-mails.

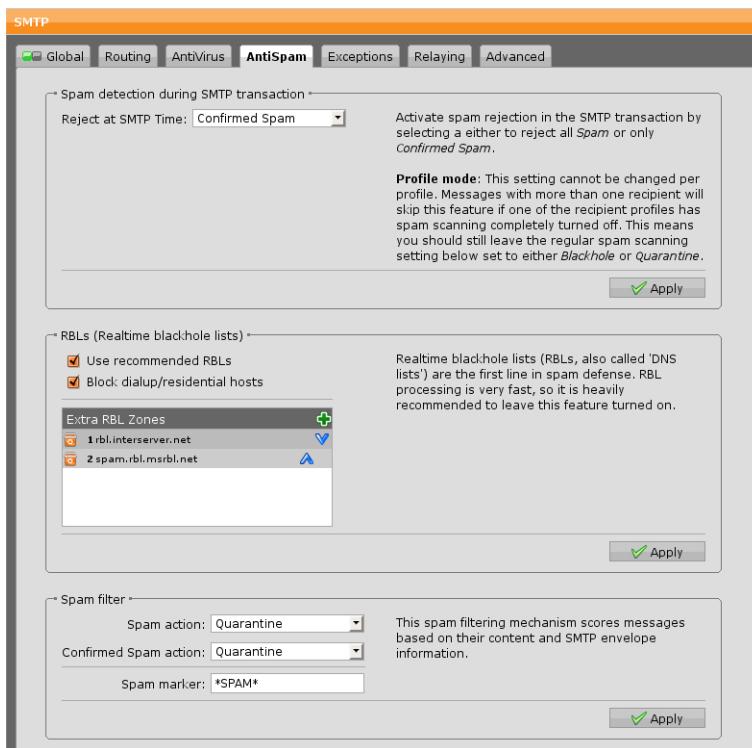


Figure 11.6 Configuring AntiSpam Settings of the SMTP Proxy

Note – The maximum size for messages to be scanned by the antispam engine of the SMTP proxy is 128 KB. Messages exceeding this size will not be scanned for spam.

Spam Detection During SMTP Transaction

You have the possibility to reject spam already during SMTP transaction. Select one of the following settings for the option *Reject at SMTP Time*:

- **Off:** Spam detection is disabled and no e-mail is going to be rejected for spam reasons.
- **Confirmed Spam:** Only confirmed spam is rejected.
- **Spam:** All e-mails that the system regards as spam are rejected. Note that there may be a higher false positive rate because e-mails regarded as probable spam may be rejected such as newsletters.

Profile Mode: This setting cannot be changed per profile. Messages with more than one recipient will skip this feature if one of the recipient profiles has spam scanning completely turned off. This means it is advisable to leave the regular spam scanning setting set to either *Spam* or *Confirmed Spam*.

RBLs (Realtime Blackhole Lists)

A *Realtime Blackhole List* (RBL) is a means by which an Internet site may publish a list of IP addresses linked to spamming.

Use recommended RBLs: Selecting this option causes the mail transfer agent to query external databases of known spam senders (so-called *Realtime Blackhole Lists*). Messages sent from a site included in one or more of such lists can easily be rejected. Several services of this type are available on the Internet. This function massively helps to reduce the amount of spam.

By default, the following RBLs are queried:

- sbl-xbl.spamhaus.org
- pbl.spamhaus.org
- cbl.abuseat.org

Note –The list of RBLs queried by Astaro Security Gateway is subject to change without notice. Astaro does not warrant for the contents of these databases.

You can also add further RBL sites to enhance the antispam capability of Astaro Security Gateway. To do so, click the plus icon in the *Extra RBL Zones* box. In the appearing textbox, enter the RBL zone and click *Apply*.

Block dial-up/residential hosts: Select this option to enable querying residential blocking lists. Residential DSL customers of Internet Service Providers (ISP) are assigned an IP address from a specific range maintained by the provider. These IP addresses may be either dynamic or static. As customers with residential IP addresses are supposed to use the ISP's mail servers and

should not be operating a mail server on their own, ISPs publish their residential IP addresses for the purpose of allowing other ISPs to refuse mail coming from those addresses. Therefore, any mail coming from an IP address listed there will be blocked if you select this option.

Click *Apply* to save changes made in this section.

Spam Filter

Astaro Security Gateway includes a heuristic check of incoming e-mails for characteristics suggestive of spam. It uses SMTP envelope information and an internal database of heuristic tests and characteristics. This spam filtering option scores messages based on their content and SMTP envelope information. Higher scores indicate a higher spam probability.

With the following two options you can specify what to do with messages that have been assigned a certain spam score. This ensures that potential spam e-mails are treated differently by the firewall.

- **Spam Action:** Here you can define what to do with messages that are classified as probable spam. Note that there may be false positives, such as newsletters, thus blackholing may lead to e-mail loss.
- **Confirmed Spam Action:** Here you can define what to do with confirmed spam messages.

You can choose between different actions for those two types of spam:

- **Off:** No messages will be marked as spam or filtered out.
- **Warn:** No messages will be filtered out. Instead, a spam flag will be added to the message's header and a spam marker will be added to the message's subject.
- **Quarantine:** The message will be blocked and stored in the e-mail quarantine. Quarantined messages can be reviewed either through the User Portal or the daily Quarantine Report.
- **Blackhole:** The message will be accepted and instantly removed.

Spam Marker: With this option you can specify a spam marker, that is, a string that will be added to the message's subject line making it easy to identify spam messages quickly. By default, the string ***SPAM*** is used to tag messages as spam.

Sender Blacklist

The envelope sender of incoming SMTP sessions will be matched against the addresses on this blacklist. If the envelope sender is found on the blacklist the

message will be blackholed.

To add a new address pattern to the blacklist click the plus icon in the *Black-listed Address Patterns* box, enter (a part of) an address, and click *Apply*. You can use an asterisk (*) as a wildcard, e.g., *@abbeybnknational.com.



Figure 11.7 Extending Sender Blacklist on AntiSpam Tab

Expression Filter

The expression filter scans messages' content passing through the SMTP proxy for specific expressions. Suspicious e-mails will be blocked. Expressions can be entered as *Perl Compatible Regular Expressions*. Simple strings such as "online dating" are interpreted in a case-insensitive manner.

Click *Apply* to save your changes.

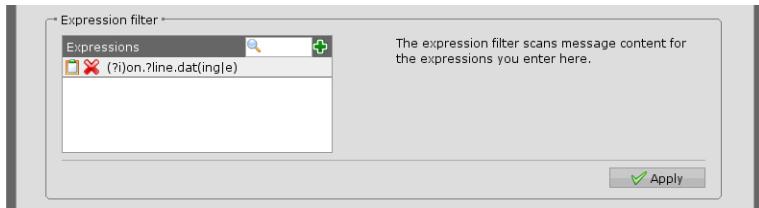


Figure 11.8 Adding Expressions to the Expression Filter on AntiSpam Tab

Advanced AntiSpam Features

This area gathers various other advanced options increasing the antispam capability of Astaro Security Gateway.

Reject Invalid HELO/Missing RDNS: Select this option if you want to reject hosts that send invalid HELO entries or lack rDNS entries. If you want to exempt hosts from this check, please refer to the *Exceptions* tab.

Use Greylisting: Greylisting basically means the temporary rejection of e-mails for a certain amount of time. Typically, a mail server using greylisting will record the following three pieces of information for all incoming messages, also known as a *triplet*.

- The sender address
- The IP address of the host the message is sent from
- The recipient address

This triplet is checked against the SMTP proxy's internal database; if the triplet has not been seen before, a record is created in the database along with a special time stamp describing it. This triplet causes the e-mail to be rejected for a period of five minutes. After that time the triplet is known to the proxy and the message will be accepted when it is sent again. Note that the triplet will expire after a week if it is not updated within this period.

Greylisting uses the fact that most senders of spam messages use software based on the "fire-and-forget" method: Try to deliver the mail and if it doesn't work, forget it! This means that senders of spam mail do not try to send e-mails again when there is a temporary failure, contrary to RFC-conform mail servers. The assumption is that since temporary failures are built into the RFC specifications for e-mail delivery, a legitimate server will try again to send the e-mail later, at which time the destination will accept it.

Use BATV: BATV is a draft of the IETF, facing the challenge to distinguish legitimate uses from unauthorized uses of e-mail addresses. BATV provides a method to sign the envelope sender of outgoing mail by adding a simple shared key to encode a hash of the address and time-varying information as well as some random data proving that the e-mail was really sent by you. It is basically used to reject bounce messages not sent by you. By using BATV, you can now check if bounces you receive are really caused by your initial e-mail, and not from a spammer forging an e-mail with your address. If a bounce returns and the e-mail address is not signed according to BATV, the SMTP proxy will not accept the message. Note that the signature provided by BATV expires after seven days. To change the key (also known as *BATV secret*) that is used to encode the hash of an e-mail's envelope MAIL FROM address, go to the *Mail Security >> SMTP >> Advanced* tab.

Note – Some mail transfer agents may reject a message whose envelope sender address was modified using BATV. In this case, you need to create an exception rule for the senders, recipients, or domains affected.

Perform SPF check: SPF (*Sender Policy Framework*) is a framework where domain owners can publish information about their outgoing e-mail servers. Domains use public records to direct requests for different services (web, e-mail, etc.) to the machines that perform those services. All domains already

publish MX records for e-mail related services to let others know what machines receive mail for the domain. SPF works by domains publishing some sort of "reverse MX" records to tell the world what machines send mail from the domain. When receiving a message from a certain domain, the recipient can check those records to make sure that mail is coming from where it should be coming from.

Cross Reference – Further information is available at the Sender Policy Framework²⁸ website.

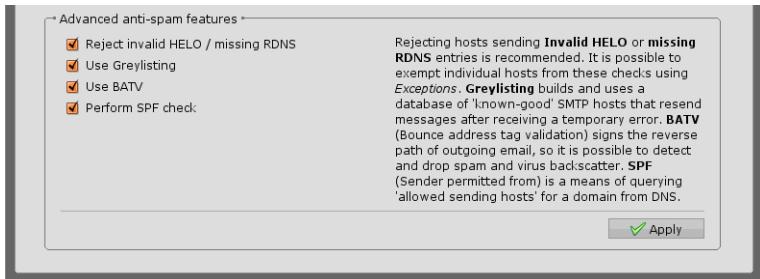


Figure 11.9 Advanced AntiSpam Features on AntiSpam Tab

As an additional antispam feature, the SMTP proxy tacitly checks each recipient address it receives with your backend mail server(s) before accepting mail for this address. E-mails for invalid recipient addresses will not be accepted. In order for this function to work, your backend mail server(s) must reject mails for unknown recipients at the SMTP stage. The general rule is that if your backend server rejects a message, the SMTP proxy will reject it, too.

Note, however, that recipient verification is *not* done for trusted (authenticated) or relay hosts, because some user agents may encounter problems when recipients get rejected in the SMTP transaction. In the usual scenario (backend mail server rejects unknown recipients in the SMTP transaction), Astaro Security Gateway will only generate bounces in the following cases:

- When a trusted or relay source sends a message to an undeliverable recipient.
- When the backend mail server has been down so that Astaro Security Gateway was not able to verify the recipient.

²⁸ <http://www.openspf.org/>

However, Astaro Security Gateway does not prevent your backend mail server(s) from sending non-delivery reports (NDRs) or bounces. In addition, Astaro Security Gateway caches positive callout replies from the mail server for 24 hours, and negative ones for two hours.

Exceptions

On the *SMTP >> Exceptions* tab you can define whitelist hosts, networks, senders, and recipients that can be excluded from antispam, antivirus, or other security checks.

Note – Since e-mails can have many recipients, and Astaro Security Gateway implements inline scanning for the SMTP protocol, scanning of an e-mail is skipped for all recipients if one of the e-mail's recipients is listed in the *Recipients* box.

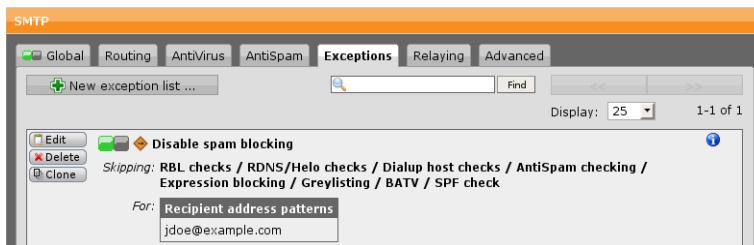


Figure 11.10 SMTP Exceptions List

To create an exception rule, proceed as follows:

1. On the *Exceptions* tab, click *New Exception List*.

The *Create Exception List* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for this exception rule.

Skip These Checks: Select the security checks that should be skipped. For more information, see *Mail Security >> SMTP >> AntiVirus* and *Anti-Spam*.

For These Source Hosts/Networks: Select the source hosts/networks (i.e., the host or network messages originate from) that should skip the security checks defined by this exception rule.

Note – No exception rule needs to be created for localhost because local messages will not be scanned by default.

When selecting this option, the *Hosts/Networks* dialog box opens. You can add a host or network by either clicking the plus symbol or the folder symbol.

These Sender Addresses: Select the senders' e-mail addresses that should skip the defined security checks.

When selecting this option, the *Senders* dialog box opens. You can either enter a complete valid e-mail address (e.g., jdoe@example.com) or all e-mail addresses of a specific domain using an asterisk as wildcard (e.g., *@example.com).

Note – Use the *Senders* option with caution, as sender addresses can easily be forged.

These Recipient Addresses: Select the recipients' e-mail addresses that should skip the defined security checks.

When selecting this option, the *Recipients* dialog box opens. You can either enter a complete valid e-mail address (e.g., jdoe@example.com) or all e-mail addresses of a specific domain using an asterisk as wildcard (e.g., *@example.com).

Comment (optional): Add a description or other information about the exception rule.

3. Click **Save**.

The new exception rule appears on the *Exceptions* list.

To either edit or delete an exception rule, click the corresponding buttons.

Relying

The SMTP proxy can be used as a mail relay. A mail relay is an SMTP server configured in such a way that it allows specific users, user groups, or hosts to relay (i.e., send) e-mails through it to domains that are not local.

Upstream Host List

An upstream host is a host that forwards e-mail to you, e.g., your ISP or external MX. If you get inbound e-mail from static upstream hosts, it is necessary

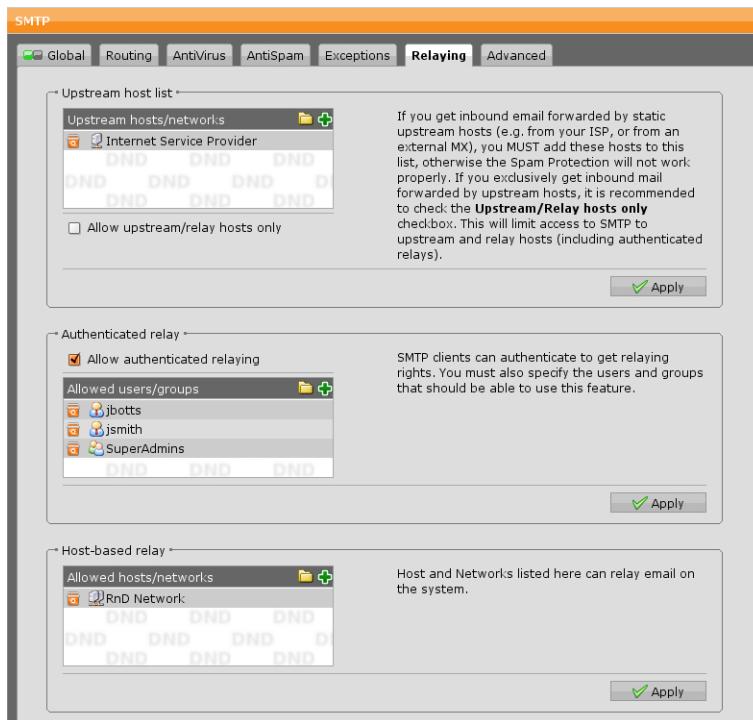


Figure 11.11 Configuring Relaying

that you enter the hosts here. Otherwise spam protection will not work properly.

To add an upstream host either click the plus icon or the folder icon for drag-and-drop from the *Networks* group tooltip. If you would like to only allow upstream hosts select the checkbox *Allow Upstream/Relay Hosts Only*. SMTP access will then be limited to the defined upstream hosts (and authenticated relays, see below). Click *Apply* to save your changes.

Authenticated Relay

SMTP clients can authenticate to get relaying privileges. Select the checkbox *Allow Authenticated Relaying* and specify the users and user groups that should be able to use this feature. Click *Apply* to save your changes.

Host-based Relay

Mail relaying can also be enabled host-based. If your local mail server or mail clients should be able to use the SMTP proxy as a mail relay, you need to add the networks and hosts which should be able to send mail through the relay to

the *Allowed Hosts/Networks* box. The networks and hosts listed are allowed to send messages to any addresses.

Caution – It is extremely important not to select Any in the *Allowed Hosts/Networks* box, because this would result in an open relay, allowing anyone on the Internet to send messages through the SMTP proxy. Spammers will quickly recognize this, leading to massive e-mail traffic. In the worst case, you will be listed on 3rd party spammer blacklists. In most configurations, the only hosts that should be allowed to relay mail are the mail servers in your network.

Click *Apply* to save your changes.

Host/Network Blacklist

Here you can define hosts and networks that shall be blocked by the SMTP proxy. Click *Apply* to save your changes.

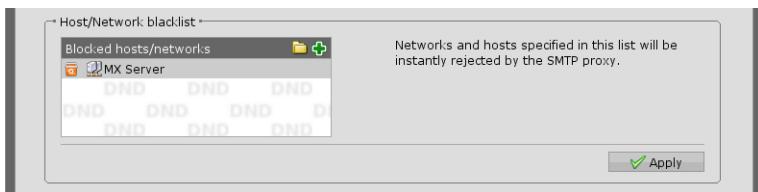


Figure 11.12 Enabling Host/Network Blacklist

Content Scan For Relayed Messages

When this option is enabled, also messages sent by either authenticated or host-based relays will be scanned for malicious content. Note that the same antivirus settings apply to relayed (outgoing) messages as for incoming messages. Click *Apply* to save your changes.

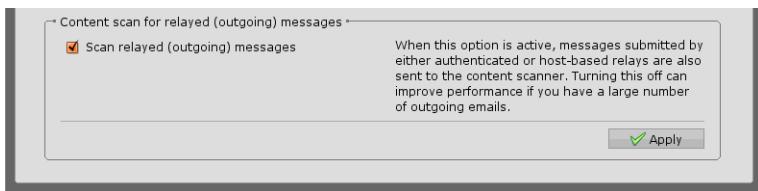


Figure 11.13 Enabling Content Scan for Relayed Messages

Advanced

On the *SMTP >> Advanced* tab you can configure additional security options of the SMTP proxy such as smarthost settings or transparent mode skip list, among others.

Parent Proxy

A parent proxy is often required in those countries that require Internet access to be routed through a government-approved proxy server. If your security policy requires the use of a parent proxy, you can set it up here by selecting the host definition and port.

Use a Parent Proxy: Select the checkbox to enable parent proxy use. Enter the hostname and the port of the proxy.

This Proxy Requires Authentication: If the parent proxy requires authentication, enter username and password here.

Transparent Mode

To enable transparent mode for SMTP select the checkbox and click *Apply*.

Hosts and networks listed in the *Skip Transparent Mode Hosts/Nets* box will not be subject to the transparent interception of SMTP traffic. However, to allow SMTP traffic for these hosts and networks, select the *Allow SMTP Traffic For Listed Hosts/Nets* checkbox. If you do not select this checkbox, you must define specific packet filter rules for the hosts and networks listed here.

TLS Settings

The security system will negotiate TLS encryption with all remote hosts supporting it. If a particular host or network should encounter problems with TLS encryption, you can enter it in the *Skip TLS Negotiation Host/Nets* box and select the appropriate TLS certificate from the drop-down menu. This will cause the security system to skip TLS negotiation for this host or network. Click *Apply* to save your settings.

DomainKeys Identified Mail (DKIM)

DKIM is a method to cryptographically sign outgoing messages. To use DKIM signing, enter your private RSA key and the corresponding key selector into the respective fields and add the domains you want to sign e-mails for to the *DKIM Domains* box. Click *Apply* to save your changes.

Confidentiality Footer

For each outgoing e-mail, you can add and customize a confidentiality footer informing users, for example, that the e-mail may contain confidential or privileged information. However, the confidentiality footer will not be appended to the e-mail if the e-mail is a reply (i.e. having a *In-Reply-To* header) or if the content type of the e-mail could not be determined.

Note – Adding a footer to messages already signed or encrypted by an e-mail client (e.g., Microsoft’s Outlook or Mozilla’s Thunderbird) will break their signature and render them invalid. If you want to create digital signatures on the client side, disable the confidentiality footer option. However, if you do not wish to forgo the privacy and authentication of your e-mail communication and still want to apply a general confidentiality footer, consider using the built-in feature of Astaro Security Gateway. E-mail encryption done on the gateway means that the footer is added to the message prior to creating the digital signature, thus leaving the signature intact.

Advanced Settings

Here you can configure the SMTP hostname and the postmaster address, among other things.

SMTP Hostname: Setting the SMTP hostname will cause the proxy to use the specified name in HELO and SMTP banner messages. By default, the normal system hostname is selected.

Postmaster Address: Specify the e-mail address of the postmaster of the security system to whom messages are to be forwarded that are sent in the form of `postmaster@[192.168.16.8]`, where the IP literal address is one of the IP addresses of the security system. Accepting such messages is an RFC requirement.

BATV Secret: Here you can change the automatically generated BATV secret used by the SMTP proxy. The BATV secret is a shared key used to sign an e-mail’s envelope `MailFrom` address, thus enabling detection of invalid bounce addresses. If you are using several MXs for your domains, you can change the BATV secret to be the same on all systems.

Max Message Size: The maximum message size that is accepted by the proxy. This setting applies to both incoming and outgoing e-mails. If your backend server has a limitation with regard to message sizes, you should set the same or a lower value here.

Max Connections: The maximum number of concurrent connections the proxy allows. Default is 20.

Max Connections/Host: The maximum number of hosts per connection the proxy allows. Default is 10.

Max Mails/Connection: The maximum number of mails per connection the proxy allows. Default is 1000.

Max Rcpt/Mail: The maximum number of recipients per mail the proxy allows. Default is 500.

Footers Mode: Here you can define how footers will be added to mails. *MIME*

Part will add the footer as extra MIME part. Existing part encodings are not changed and national language characters are preserved. The other method is *Inline* which means that the footer is separated from the main mail by the - separator. With this mode you can choose whether the footer should be Unicode (UTF-8) converted or not. Unicode conversion upgrades the message to preserve national language characters in the footer.

Smarthost Settings

A smarthost is a type of mail relay server which allows an SMTP server to route mail to an upstream mail server rather than directly to the recipient's server. Often this smarthost requires authentication from the sender to verify that the sender has privileges to have mail forwarded through the smarthost.

Use A Smarthost: If you want to use a smarthost to send mail, select the checkbox and enter the hostname or IP address of the smarthost. You may also add a port number, separated from the IP address by a colon, e.g., 195.99.144.85:443. In that case, the proxy will never deliver mail itself, but rather send anything to the smarthost. If the smarthost requires authentication, select the *This Smarthost Requires Authentication* checkbox and enter a username and password in the respective fields. Both *Plain* and *Login* authentication types are supported.

SMTP Profiles

The SMTP proxy of Astaro Security Gateway lets you create alternative SMTP profiles, which can then be associated with different domains. That way you can specify domains that should use a different profile other than the default profile configured in *Mail Security >> SMTP*. The order of the functions, structured as tabs, reflects how each step gets processed one after the other during SMTP time.

To create an SMTP profile, proceed as follows:

- 1. Enable the SMTP profile mode.**

On the *Mail Security >> SMTP >> Global* tab select *Profile Mode* and click *Apply*.

The SMTP profiles creation in the *Mail Security >> SMTP Profiles* menu is enabled.

- 2. On the *SMTP Profiles* tab, click *Create New Profile*.**

A dialog box opens.

- 3. Enter a descriptive name for the profile and click *OK*.**

The settings page for the profile opens.

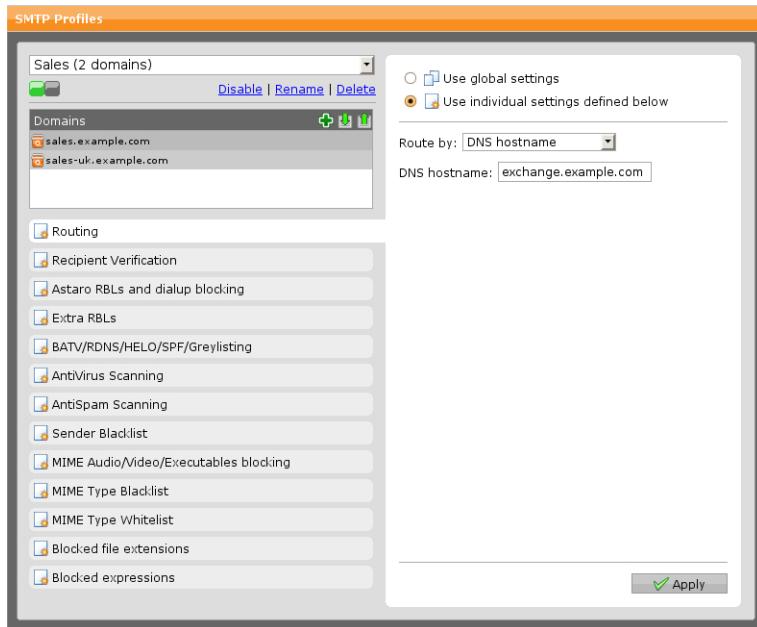


Figure 11.14 Configuring an SMTP Profile

4. **Add one or more domains.**

Add one or more domains to the *Domains* box.

Settings of this profile will be applied for those domains.

5. **Make the following settings:**

You only need to make settings for functions you want to use. For each of the following functions you can decide whether to use individual settings defined here or global settings defined under *Mail Security >> SMTP*. By default, the individual settings option is selected. The individual settings for each function are described below.

Note – Encrypted e-mails whose sender addresses include a domain name configured here cannot be decrypted when using the e-mail encryption/decryption engine of Astaro Security Gateway. Therefore, no profile should be added for external e-mail domains.

All settings that you can define here can also be set globally in *Mail Security >> SMTP*. Therefore only a list of settings and the differences from the global settings are given here, along with cross-references to the respective global setting where detailed information can be found.

The following settings can be made:

- **Routing:** On the *Routing* tab you can configure domain and routing targets for the SMTP proxy and define how recipients shall be verified.

- Static Host List
- DNS Hostname
- MX Records

For detailed information please refer to *Mail Security >> SMTP >> Routing*.

- **Recipient verification**

Verify recipients: Here you can specify whether and how e-mail recipients are to be verified.

- **With Callout:** A request is sent to the server to verify the recipient.
- **In Active Directory:** A request is sent to the Active Directory server to verify the recipient. To be able to use Active Directory you must have an Active Directory server specified in *Users >> Authentication >> Servers*. Enter a Base DN into the *Alternative Base DN* field.

Note – The use of Active Directory recipient verification may lead to bounced messages in case the server does not respond.

- **Off:** You can turn off recipient verification completely but this is not recommended for it will lead to higher spam traffic volume and dictionary attacks. Thus your quarantine is likely to be flooded with unsolicited messages.

For detailed information please refer to *Mail Security >> SMTP >> Routing*.

- **Astaro RBLs and Dial-up Blocking:** Here you can block IP addresses linked to spamming.

- Use Recommended RBLs
- Block Dial-up/Residential Hosts

For detailed information please refer to *Mail Security >> SMTP >> AntiSpam*.

- **Extra RBLs:** You can add further RBL sites to enhance the antispam capability of Astaro Security Gateway. For detailed information please refer to *Mail Security >> SMTP >> AntiSpam*. Note that, as a third option, you can add the global settings to your individual settings here.
- **BATV/RDNS/HELO/SPF/Greylisting:** This tab gathers various other advanced options increasing the antispam capability of Astaro Security Gateway.
 - Reject Invalid HELO/Missing RDNS
 - Use Greylisting
 - Use BATV
 - Perform SPF Check
- **AntiVirus Scanning:** You can configure how to proceed with messages that contain malicious content. The following actions are available:
 - Off
 - Quarantine
 - Blackhole

You can choose between the following antivirus scan options:

- Single Scan: Provides maximum performance.
- Dual Scan: Provides maximum security.

Quarantine Unscannable and Encrypted Content: Select this option to quarantine e-mails whose content could not be scanned. The reason for that may be, among other things, that content is encrypted or corrupt.

For detailed information please refer to *Mail Security >> SMTP >> AntiVirus*.

- **AntiSpam Scanning:** Here you can decide how to deal with unsolicited commercial e-mails. Both for spam and confirmed spam you can choose between the following actions:

- Off
- Warn
- Quarantine
- Blackhole

For detailed information please refer to *Mail Security >> SMTP >> AntiSpam*.

- **Sender Blacklist:** The envelope sender of incoming SMTP sessions will be matched against the addresses on this blacklist. If the envelope sender is found on the blacklist the message will be blackholed. For detailed information please refer to *Mail Security >> SMTP >> Anti-Spam*. Note that, as a third option, you can add the global settings to your individual settings here.

- **MIME Audio/Video/Executables Blocking:** The MIME type filter reads the MIME type of e-mail contents. You can select which content types you would like to quarantine:

- Audio Content
- Video Content
- Executable Content

For detailed information please refer to *Mail Security >> SMTP >> AntiVirus*.

- **MIME Type Blacklist:** Here you can add additional MIME types to quarantine. For detailed information please refer to *Mail Security >> SMTP >> AntiVirus*. Note that, as a third option, you can add the global settings to your individual settings here.

- **MIME Type Whitelist:** Here you can add MIME types not to quarantine. For detailed information please refer to *Mail Security >> SMTP >> AntiVirus*. Note that, as a third option, you can add the global settings to your individual settings here.

- **Blocked File Extensions:** Using the *File Extension Filter* you can quarantine e-mails (with warnings) that contain certain types of files based on their extensions (e.g., executables). For detailed information please refer to *Mail Security >> SMTP >> AntiVirus*. Note that, as a third option, you can add the global settings to your individual settings here.
- **Blocked Expressions:** The expression filter scans messages' content passing through the SMTP proxy for specific expressions. Suspicious e-mails will be blocked. For detailed information please refer to *Mail Security >> SMTP >> AntiSpam*. Note that, as a third option, you can add the global settings to your individual settings here.

6. Click *Apply*.

Your settings will be saved. The new profile appears on the *SMTP Profiles* list.

Note – When you select *Use Global Settings* for a topic and click *Apply*, the icon of the function changes to the global settings icon. By this, you can easily get an overview on which functions global settings or individual settings are applied.

To either disable, rename or delete a profile click the corresponding buttons at the top below the profile drop-down list.

POP3

The menu *Mail Security >> POP3* lets you configure the POP3 proxy for incoming e-mails. The *Post Office Protocol 3* (POP3) is an application-layer Internet standard protocol that allows the retrieval of e-mails from a remote mail server. The POP3 proxy works transparently, meaning that all POP3 requests coming from the internal network on port 110 are intercepted and redirected through the proxy invisible to the client. The advantage of this mode is that no additional administration or client-side configuration is necessary.

Note – It might be necessary to increase the server timeout settings in the e-mail clients' configuration. Usual default settings of about one minute or less might be too low, especially when fetching large e-mails.

The POP3 protocol does not have server-side tracking of which mails have already been retrieved. Generally, a mail client retrieves a mail and deletes it on the server afterwards. However, if the client is configured to not delete mails, then server-side deleting is omitted and the client keeps track of which mail has already been fetched.

Global

On the *Mail Security >> POP3 >> Global* tab you can configure basic settings for the POP3 proxy.

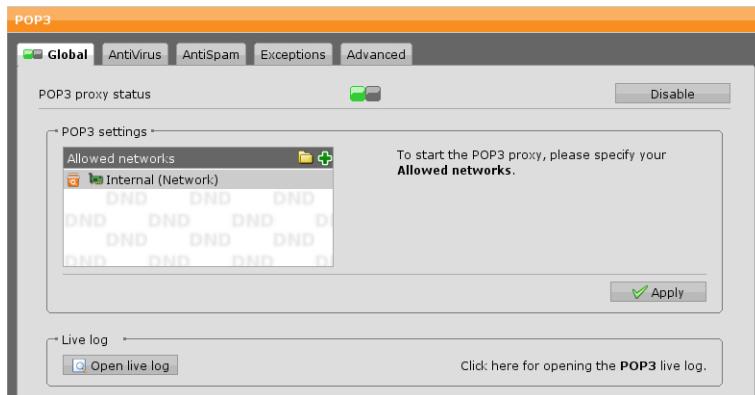


Figure 11.15 Configuring the POP3 Proxy

To configure the POP3 proxy, proceed as follows:

1. Enable the POP3 proxy.

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *POP3 Settings* area becomes editable.

2. Select the allowed networks.

Select the networks that should be allowed to proxy POP3 traffic. By default, this is the internal network.

3. Click *Apply*.

Your settings will be saved.

To cancel the configuration, click *Abort Enable* or the amber colored status icon.

Live Log

The *POP3 Live Log* logs the POP3 proxy activities, showing all incoming e-mails. Click the button to open the live log in a new window.

AntiVirus

The *AntiVirus* tab contains various measures against e-mails that carry harmful and dangerous content such as viruses, worms, or other malware.

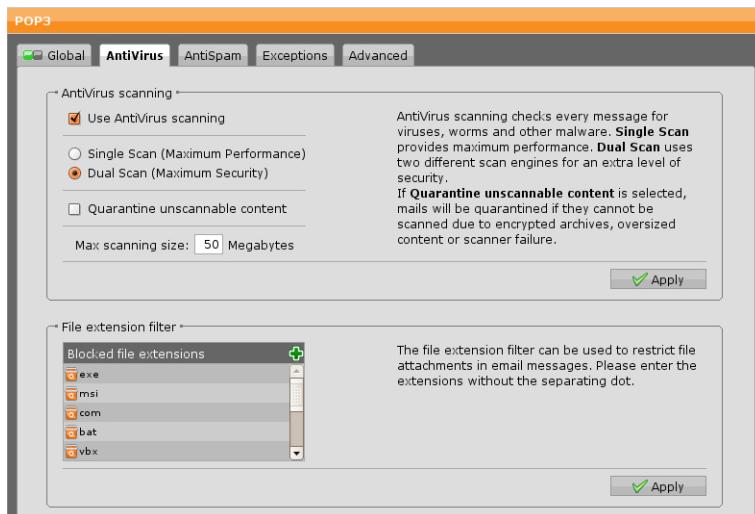


Figure 11.16 Configuring AntiVirus Settings of the POP3 Proxy

AntiVirus Scanning

When using this option, e-mails will be scanned for unwanted content such as viruses, trojan horses, or suspicious file types. Messages containing malicious content will be blocked and stored in the e-mail quarantine. Users can review and release their quarantined messages either through the Astaro User Portal or the daily Quarantine Report. However, messages containing malicious content can only be released from the quarantine by the administrator in the Mail Manager.

Astaro Security Gateway features several antivirus engines for best security.

- **Single Scan:** Default setting; provides maximum performance.
- **Dual Scan:** Provides maximum recognition rate by scanning all e-mails twice using different virus scanners.

Quarantine Unscannable and Encrypted Content: When you select this option, e-mails with content that cannot be scanned will be quarantined. Unscannable content may be encrypted or corrupt archives or oversized content, or there may be a technical reason like a scanner failure.

Max Scanning Size: Specify the maximum size of messages to be scanned by the antivirus engine(s). Messages exceeding this size will be exempt from scanning.

Click *Apply* to save your settings.

File Extension Filter

This feature filters e-mails that contain file attachments of a certain extension (e.g., executable binaries) from web traffic that have a file extension listed in the *Blocked File Extensions* box. You can add additional file extensions or delete file extensions that are not to be blocked. To add a file extension, click the plus icon in the *Blocked File Extensions* box and enter the file extension you want to block, for example `exe` (without the delimiting dot). Click *Apply* to save your settings.

Note – Encrypted `zip` archives cannot be scanned for malicious content and will pass through the virus scanner. To protect your network from malware included in encrypted `zip` files you might want to consider blocking the `zip` file extension altogether.

AntiSpam

Astaro Security Gateway can be configured to detect unsolicited spam e-mails and to identify spam transmissions from known or suspected spam purveyors. Configuration options located on the *AntiSpam* tab let you configure POP3 security features aimed at preventing your network from receiving unsolicited commercial e-mails.

Note – The maximum size for messages to be scanned by the antispam engine of the POP3 proxy is 128kB. Messages exceeding this size will not be scanned for spam.

Spam Filter

Astaro Security Gateway includes a heuristic check of incoming e-mails for characteristics suggestive of spam. It uses SMTP envelope information and an

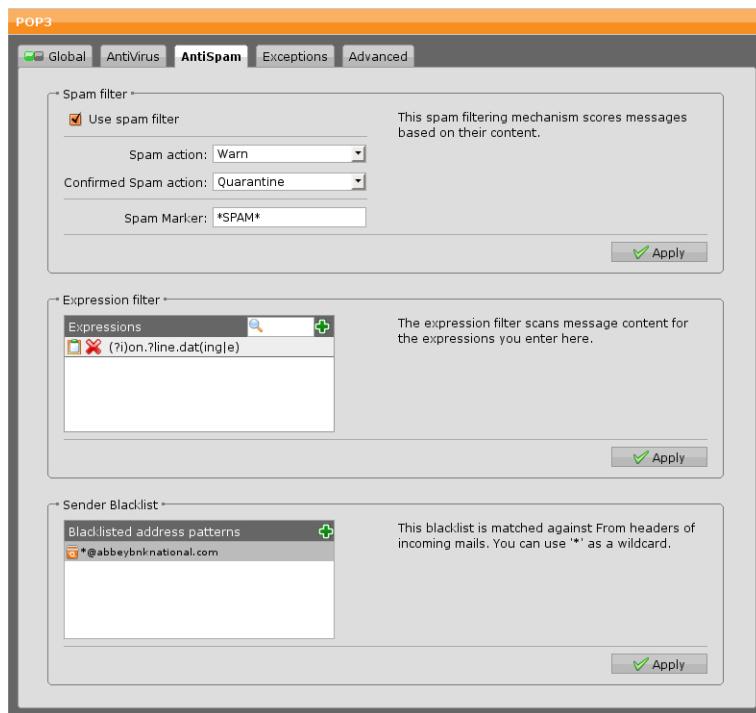


Figure 11.17 Configuring AntiSpam Settings of the POP3 Proxy

internal database of heuristic tests and characteristics. This spam filtering option scores messages based on their content and SMTP envelope information. Higher scores indicate a higher spam probability.

With the following two options you can specify what to do with messages that have been assigned a certain spam score. This ensures that potential spam e-mails are treated differently by the firewall.

- **Spam Action:** Here you can define what to do with messages that are classified as probable spam. Note that there may be false positives, such as newsletters, thus blackholing may lead to e-mail loss.
- **Confirmed Spam Action:** Here you can define what to do with confirmed spam messages.

You can choose between different actions for those two types of spam:

- **Off:** No messages will be marked as spam or filtered out.
- **Warn:** No messages will be filtered out. Instead, a spam flag will be added to the message's header and a spam marker will be added to the message's subject.
- **Quarantine:** The message will be blocked and stored in the e-mail quarantine. Quarantined messages can be reviewed either through the User Portal or the daily Quarantine Report.

Spam Marker: With this option you can specify a spam marker, that is, a string that will be added to the message's subject line making it easy to identify spam messages quickly. By default, the string *SPAM* is used to tag messages as spam.

Expression Filter: The expression filter scans the message's subject and body for specific expressions. E-mails that contain an expression listed here will be blocked. However, if the prefetch option is enabled on the *Mail Security >> POP3 >> Advanced* tab, the e-mail will be sent to the quarantine. Expressions can be entered as *Perl Compatible Regular Expressions*. Simple strings such as "online dating" are interpreted in a case-insensitive manner.

Click *Apply* to save changes.

Sender Blacklist

The envelope sender of incoming POP3 sessions will be matched against the addresses on this blacklist. If the envelope sender is found on the blacklist the message will be quarantined and marked as *Other* in the subject line.

To add a new address pattern to the blacklist click the plus icon in the *Black-listed Address Patterns* box, enter (a part of) an address, and click *Apply*. You can use an asterisk (*) as a wildcard, e.g., *@abbeybnknational.com.

Exceptions

On the *POP3 >> Exceptions* tab you can define client hosts/networks and sender addresses that shall be excluded from various security features.

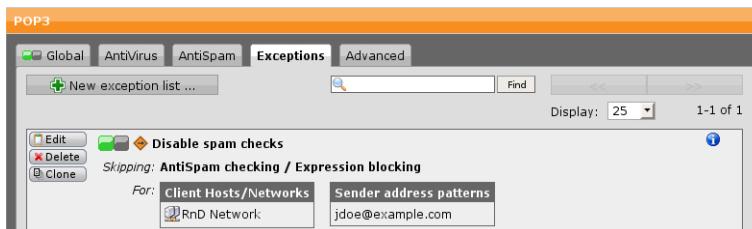


Figure 11.18 POP3 Proxy Exceptions List

To create an exception rule, proceed as follows:

1. **On the Exceptions tab, click New Exception List.**

The *Create Exception List* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for this exception rule.

Skip These Checks: Select the security checks that should be skipped. For more information, see *Mail Security >> SMTP >> AntiVirus* and *Anti-Spam*.

For These Client Hosts/Networks: Select the source hosts/networks (i.e., the hosts or networks messages originate from) that should skip the security checks defined by this exception rule.

Note – No exception rule needs to be created for localhost because local messages will not be scanned by default.

When selecting this option, the *Hosts/Networks* dialog box opens. You can add a host or network by either clicking the plus symbol or the folder symbol.

These Sender Addresses: Select the senders' e-mail addresses that should skip the defined security checks.

When selecting this option, the *Senders* dialog box opens. You can either enter a complete valid e-mail address (e.g., jdoe@example.com) or all e-mail addresses of a specific domain using an asterisk as wildcard (e.g., *@example.com).

Note – Use the *Senders* option with caution, as sender addresses can easily be forged.

Comment (optional): Add a description or other information about the exception rule.

3. **Click Save.**

The new exception rule appears on the *Exceptions* list.

To either edit or delete an exception rule, click the corresponding buttons.

Advanced

On the *POP3 >> Advanced* tab you can specify those hosts and networks that can skip the transparent mode of the POP3 proxy. In addition, it contains the POP3 proxy's prefetch option, which allows the prefetching of messages from a POP3 server and storing them in a database.

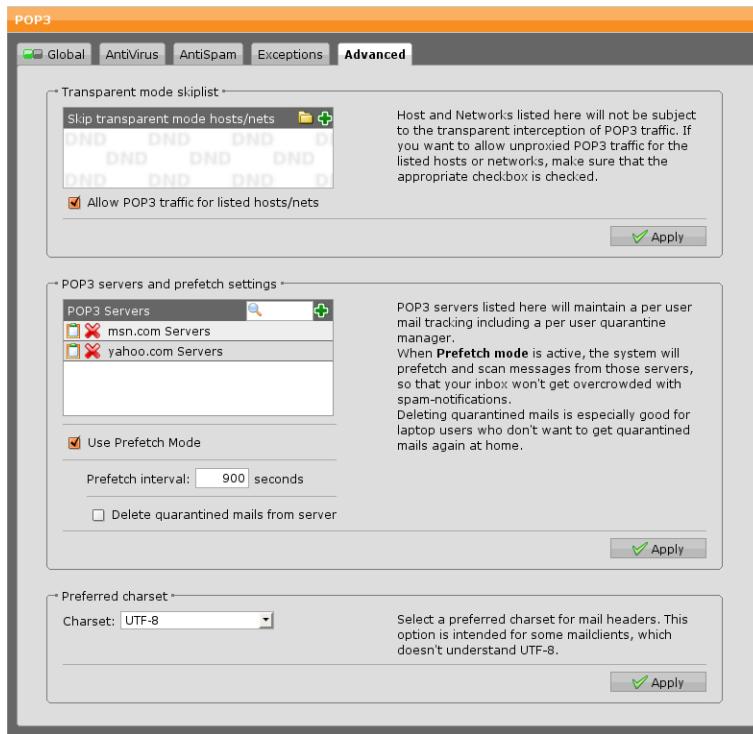


Figure 11.19 Configuring Advanced POP3 Proxy Settings

Transparent Mode Skip List

Using this option is only meaningful if the POP3 proxy runs in transparent mode. Hosts and networks listed in the *Skip Transparent Mode Hosts/Nets* box will not be subject to the transparent interception of POP3 traffic. However, to allow POP3 traffic for these hosts and networks, select the *Allow POP3 Traffic For Listed Hosts/Nets* checkbox. If you do not select this checkbox, you must define specific packet filter rules for the hosts and networks listed here.

POP3 Servers And Prefetch Settings

You can enter one or more POP3 servers here, so that they are known to the proxy. Additionally, you can turn on prefetching.

POP3 Servers: Specify the POP3 servers that are used in your network or by your end-users.

If no POP3 server is specified and a mail gets caught by the proxy, the proxy replaces the mail with a notification to the recipient right away in the same connection stating that the mail has been quarantined. The quarantined mail can be viewed in *Mail Manager*, but is not associated to a server or account and therefore cannot be released in a later connection. Generally, releasing of e-mails from quarantine does only work for prefetched messages.

There are two scenarios:

- If POP3 server(s) are given and prefetching is disabled, the proxy keeps track which quarantined mails belong to which server/account. Thus, quarantined mail can be released when the client polls the mailbox next time. For this to work, the proxy has to safely identify which ip addresses belong to which server (by their FQDN which you have entered in your mail client).
- If POP3 server(s) are given and prefetching is enabled, the POP3 proxy periodically checks the POP3 server(s) for new messages. If a new message has arrived, it will be copied to the POP3 proxy, scanned and stored into a database on the security system. The message remains on the POP3 server. When a client tries to fetch new messages, it communicates with the POP3 proxy instead and only retrieves messages from this database.

A POP3 proxy supporting prefetching has a variety of benefits, among others:

- No timeout problems between client and proxy or vice versa.
- Delivery of messages is much faster because e-mails have been scanned in advance.
- Blocked messages can be released from the User Portal—they will then be included in the next fetch.

If a message was blocked because it contained malicious content or because it was identified as spam, it will not be delivered to the client. Instead, such a message will be sent to the quarantine. A message held in quarantine is stored in the *Mail Manager* section of the User Portal, from where it can be deleted or released.

Use Prefetch Mode: To enable prefetch mode, select the checkbox and add one or more POP3 servers to the *POP3 Server* box.

Prefetch Interval: Select the time interval at which the POP3 proxy contacts the POP3 server to prefetch messages.

Note – The interval at which mail clients are allowed to connect to the POP3 server may vary from server to server. The prefetch interval should therefore not be set to a shorter interval than allowed by the POP3 server, because otherwise the download of POP3 messages would fail as long as the access to the POP3 server is blocked.

Note further that several mail clients may query the same POP3 account. Whenever messages were successfully fetched from a POP3 server, this will restart the timer until the server can be accessed for the next time. If for that reason the POP3 proxy cannot access a POP3 server four times in a row (default is every 15 minutes), the account password will be deleted from the proxy's mail database and no e-mails will be fetched until a mail client sends the password to the POP3 server again and successfully logs in.

Delete Quarantined Mails From Server: When you select this option, quarantined messages will be deleted from the POP3 server immediately. This is useful to prevent that users get spam or virus messages when they connect to the POP3 server not via the ASG, but for example via the POP3 server's web portal.

If the e-mail client is configured to delete messages from the server after retrieving them, this information will be stored in the database, too. The next time the proxy is going to prefetch messages for this POP3 account, it will delete the messages from the server. This means, as long as no client fetches the messages from the Astaro Security Gateway *and* no delete command is configured, no message will be deleted from the POP3 server. Therefore, they can still be read, for example, via the web portal of the e-mail provider.

Quarantined messages are deleted from the POP3 server in the following cases:

- Messages are manually deleted via the Mail Manager.
- Messages are manually deleted by the user via the User Portal.
- The message was released (either through the Quarantine Report or the User Portal) and the user's e-mail client is configured to delete messages upon delivery.

- The notification message has been deleted.
- After the storage period has expired (see section *Configuration* in chapter *Mail Manager*).

In prefetch mode however, spam messages in quarantine cannot be deleted from the POP3 server directly by means of a client command.

Note – The e-mail client must successfully connect to the POP3 server at least once for the prefetch function to operate properly. This is because Astaro Security Gateway needs to store the name of the POP3 server, the username, and the user's password in a database in order to fetch POP3 messages on behalf of this user. This, however, *cannot* be achieved by configuring POP3 account credentials in the Astaro User Portal (for more information, see User Portal). The POP3 account credentials in the User Portal are needed for prefetched messages to appear in this user's portal and daily Quarantine Report.

SSL is currently not supported, therefore mails from mail providers such as googlemail, which offer SSL-only access, cannot be filtered by the proxy.

Note for fetchmail users: The TOP method is not supported to download e-mails from the mail server for security reasons—messages that are received through TOP cannot be scanned. It will work if you specify the fetchall option (-a on command line). For more information please read "RETR or TOP" in the fetchmail manual.

Preferred Charset

In this section you can select a charset different than UTF-8 that will subsequently used for mail headers. This is useful if your users use mail clients which do not understand UTF-8.

Encryption

Ever since e-mail became the primary electronic communication medium for personal and business purposes, a legitimate concern over privacy and authentication has arisen. In general terms, the e-mail format is transmitted in clear text, similar to a postcard which anyone could read. Moreover, as assimilating false identities is an easy process, it is important for the recipient to be able to tell if the sender is who they claim to be.

Solutions to these issues are typically accomplished with e-mail encryption and digital certificates, where an e-mail message is electronically signed and cryptographically encoded. This assures that the message recipient exclusively can

open and view the contents of the e-mail (privacy), verifying the identity of the sender (authentication). In other words, this process negates the idea of being sent an "e-postcard", and introduces a process much like registered or certified mail.

Modern cryptography has two methods to encrypt e-mail: symmetric and asymmetric. Both have become standard methods and are utilized in several types of applications. Symmetric key cryptography refers to encryption methods in which both, the sender and receiver, share the same key.

On the other hand, asymmetric key cryptography (also known as public key cryptography) is a form of cryptography in which each user has a pair of cryptographic keys; a public key, which encrypts data, and a corresponding private or secret key for decryption. Whereas the public key is freely published, the private key will be securely kept by the user.

One drawback with symmetric encryption is that for a sender and recipient to communicate securely, they must agree upon a key and keep it secret between themselves. If they are in different physical locations, they must prevent the disclosure of the secret key during transmission. Therefore, the persistent problem with symmetric encryption is key distribution: how do I get the key to the recipient without someone intercepting it? Public key cryptography was invented to exactly address this problem. With public key cryptography, users can securely communicate over an insecure channel without having to agree upon a shared key beforehand.

The need for e-mail encryption has produced a variety of public key cryptography standards, most notably S/MIME and OpenPGP, both of which are supported by Astaro Security Gateway. S/MIME (*Secure Multipurpose Internet Mail Extensions*) is a standard for asymmetric encryption and the signing of e-mails encapsulated in MIME. It is typically used within a public key infrastructure (PKI) and is based on a hierarchical structure of digital certificates, requiring a trusted instance as Certification Authority (CA). The CA issues a digital certificate by binding an identity to a pair of electronic keys; this can be seen as a digital counterpart to a traditional identity document such as a passport. Technically speaking, the CA issues a certificate binding a public key to a particular *Distinguished Name* in the X.500 standard, or to an *Alternative Name* such as an e-mail address.

A digital certificate makes it possible to verify someone's claim that they have the right to use a given key. The idea is that if someone trusts a CA and can verify that a public key is signed by this CA, then one can also be assured that the public key in question really does belong to the purported owner.

OpenPGP (*Pretty Good Privacy*), on the other hand, uses asymmetric encryption typically employed in a *web of trust* (WOT). This means that public keys are digitally signed by other users who, by that act, endorse the association of that public key with the person.

Note – Although both standards offer similar services, S/MIME and OpenPGP have very different formats. This means that users of one protocol cannot communicate with the users of the other. Furthermore, authentication certificates also cannot be shared.

The entire e-mail encryption is transparent to the user, that is, no additional encryption software is required on the client side. Generally speaking, encryption requires having the destination party's certificate or public key on store. For incoming and outgoing messages, e-mail encryption functions as follows:

- By default, outgoing messages from internal users will be scanned, automatically signed, and encrypted using the recipient's certificate (S/MIME) or public key (OpenPGP), provided the S/MIME certificate or OpenPGP public key of the recipient is existent on the security system.
- Encrypted incoming messages from external users whose S/MIME certificate or OpenPGP public key are known to the security system will automatically be decrypted and scanned for malicious content. To decrypt the message, the S/MIME key or OpenPGP private key of the internal user must be existent on the security system.
- Encrypted incoming messages from external users or for internal users unknown to the security system will be delivered, although they cannot be decrypted and therefore not scanned for viruses or spam. It is then the responsibility of the recipient (internal user) to ensure that the e-mail does not contain any malware, for example, by using a personal firewall.
- Outgoing messages already encrypted on the client side will directly be sent to the recipient if the recipient's S/MIME certificate or OpenPGP public key are unknown. However, if the recipient's S/MIME certificate or OpenPGP public key are available, the message will be encrypted a second time. Note that pre-encrypted messages cannot be scanned for malicious content.
- Decryption is only possible for incoming e-mails, where "incoming" means that the domain name of the sender's e-mail address must not be part of any SMTP profile. For example, to decrypt a message sent by

`jdoe@example.com`, the domain `example.com` must *not* be configured in either the routing settings or any SMTP profile.

- A summary of the signing/encryption result is written into the subject line of each e-mail. For example, an e-mail that was correctly signed and encrypted with S/MIME, has "(S/MIME: Signed and encrypted)" appended to the subject line.

Note – Adding a footer to messages already signed or encrypted by an e-mail client (e.g., Microsoft's Outlook or Mozilla's Thunderbird) will break their signature and render them invalid. If you want to create digital signatures on the client side, disable the antivirus check footer and confidentiality footer options, which are located on the *Mail Security >> SMTP >> AntiVirus* and *Mail Security >> SMTP >> Advanced* tabs, respectively. However, if you do not wish to forgo the privacy and authentication of your e-mail communication and still want to apply general footers, consider using the built-in feature of Astaro Security Gateway. E-mail encryption done on the gateway means that the footer is added to the message prior to creating the digital signature, thus leaving the signature intact.

Global

On the *Mail Security >> Encryption >> Global* tab you can configure the basic settings of the e-mail encryption functionality.

Cross Reference – For a comprehensive description of how to use e-mail encryption, see the E-Mail Encryption Guide, which is available at Astaro's knowledgebase²⁹ (navigate to *ASG Version 7 >> Astaro Manuals and Guides*).

Note – Encryption is only working for SMTP, not for POP3.

Before you can use e-mail encryption, you must first create a *Certificate Authority* (CA) consisting of a CA certificate and CA key. The CA certificate can be downloaded and stored locally. In addition, it can be installed as an external

²⁹ <http://www.astaro.com/kb>

CA (S/MIME Authority) in other units as illustrated in the diagram to enable transparent e-mail encryption between two Astaro Security Gateway units.

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

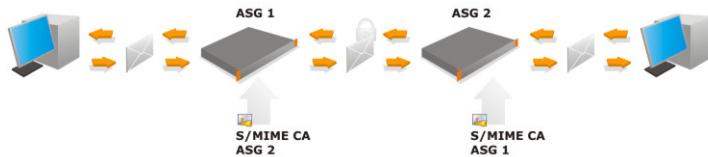


Figure 11.20 E-mail Encryption Using Two Astaro Security Gateway Units



Figure 11.21 Configuring E-mail Encryption

To configure e-mail encryption, proceed as follows:

1. **On the *Global* tab, enable e-mail encryption.**

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *E-mail Encryption Certificate Authority (CA)* area becomes editable.

2. **Create a certificate authority (CA).**

Fill out the form in the *Email Encryption Certificate Authority (CA)* area.

By default, the form is filled out with the values of the *Management >> System Settings >> Organizational* tab.

3. Click Save.

The status icon turns green and the following certificates and keys are being created:

- S/MIME CA Certificate
- OpenPGP Postmaster Key

Note that this may take several minutes to complete. If you do not see the fingerprints of the S/MIME CA certificate or the Open PGP Postmaster key, click the *Reload* button in the upper right corner of WebAdmin. The certificate and the key can be downloaded and locally stored.

Use the *Reset E-mail Encryption System Now* button to reset all settings in the *E-mail Encryption* menu to the factory default configuration.

Options

On the *Encryption >> Options* tab you can define the default policy to be used within the public key cryptography framework of Astaro Security Gateway.

Encryption

Global Options Internal Users S/MIME Authorities S/MIME Certificates OpenPGP Public Keys

Default policy

Sign outgoing email
 Encrypt outgoing email
 Verify incoming email
 Decrypt incoming email

These options define the default policy for signing, en- and decrypting email. It is possible to override the default policy on a per-user basis.

Enable automatic S/MIME certificate extraction

When this option is enabled, the email encryption system will automatically extract S/MIME certificates from incoming email traffic if the certificates are signed with a valid S/MIME authority.

OpenPGP Keyserver

gpgkeys.mit.edu

Optional Keyserver for OpenPGP. You can append a port number to the hostname, separated with a colon.

Figure 11.22 E-mail Encryption Options

Default Policy: Specify your default policy for e-mails in terms of cryptography. These settings can, however, be overwritten by customized settings.

The following actions can be selected:

- Sign outgoing e-mail
- Encrypt outgoing e-mail
- Verify incoming e-mail
- Decrypt incoming e-mail

Confirm your settings by clicking *Apply*.

Note – For encryption to work, the sender must be within the Internal Users list. Outgoing e-mails for recipients whose S/MIME certificate or OpenPGP public key are existent on the firewall will be encrypted by default. If you want to disable encryption for these recipients, delete their S/MIME certificates or OpenPGP public keys. If certificates or public keys are unknown to the security system, e-mails will be sent unencrypted.

Automatic Extraction of S/MIME Certificates

When this option is selected, S/MIME certificates will automatically be extracted from incoming e-mails provided the certificate that is appended to the e-mail is signed by a trusted certificate authority, that is, a CA present on the unit as shown on the *Mail Security >> Encryption >> S/MIME Authorities* tab. In addition, the time and date of Astaro Security Gateway must be within the certificate's validity period for the automatic extraction of certificates to work. Once a certificate has been successfully extracted, it will appear on the *Mail Security >> Encryption >> S/MIME Certificates* tab. Note that this may take five to ten minutes to complete.

Click *Apply* to save changes.

OpenPGP Keyserver

OpenPGP keyserver host public PGP keys. You can add an OpenPGP keyserver here. For encrypted incoming e-mails and for outgoing e-mails that shall be encrypted, the ASG will try to retrieve the public key from the given server if the respective public key is yet unknown to the ASG.

Internal Users

For signing and decrypting messages, either the S/MIME key or the OpenPGP private key must be existent on the security system. On the *Encryption >>*

Internal Users tab you can create both an individual S/MIME key/certificate and/or OpenPGP key pair for those users for whom e-mail encryption should be enabled.

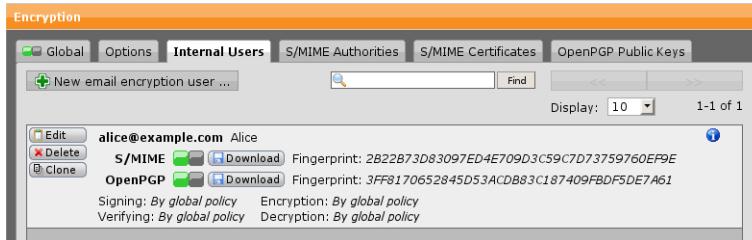


Figure 11.23 Internal Users List

To create an internal e-mail user, proceed as follows:

1. On the **Internal Users** tab, click **New Email Encryption User**.

The *Create New User* dialog box opens.

2. Make the following settings:

E-mail Address: Enter the e-mail address of the user.

Full Name: Enter the name of the user.

Signing: The following signing options are available:

- Use Default Policy: The policy from the *Options* tab will be used.
- On: E-mails will be signed using the certificate of the user.
- Off: E-mails will not be signed.

Encryption: The following encryption options are available:

- Use Default Policy: The policy from the *Options* tab will be used.
- On: E-mails will be encrypted using the public key of the recipient.
- Off: E-mails will not be encrypted.

Verifying: The following verification options are available:

- Use Default Policy: The policy from the *Options* tab will be used.
- On: E-mails will be verified using the public key of the sender.
- Off: E-mails will not be verified.

Decryption: The following decryption options are available:

- Use Default Policy: The policy from the *Options* tab will be used.
- On: E-mails will be decrypted using the certificate of the user.
- Off: E-mails will not be decrypted.

S/MIME: Select whether you want to have the S/MIME certificate and key automatically generated by the system or whether you want to upload a certificate in PKCS#12 format. When uploading the certificate, you must know the passphrase the PKCS#12 file was protected with. Note that the PKCS#12 file must both contain the S/MIME key and certificate. Any CA certificate that may be included in this PKCS#12 file will be ignored.

OpenPGP: Select whether you want to have the OpenPGP key pair consisting of a private key and the public key automatically generated by the system or whether you want to upload the key pair in ASCII format. Note that both private and public key must be included in one single file and that the file must not contain a passphrase.

Note – If you configure both S/MIME and OpenPGP for an individual user, e-mails sent by this user will be signed and encrypted using S/MIME.

Comment (optional): Add a description or other information about the internal user.

3. Click **Save**.

The new user appears on the *Internal Users* list.

Use the status icon to turn the usage of one or both keys off without having to delete the key(s).

Note – For security reasons, the files offered for download only contain the S/MIME certificate and the OpenPGP public key, respectively. The S/MIME key and the OpenPGP private key cannot be downloaded from the system. To avoid problems with file downloads using Internet Explorer 6, add the URLs of the firewall (e.g., <https://192.168.2.100>) and User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

S-MIME Authorities

On the *Encryption >> S/MIME Authorities* tab, import the certificate (i.e., the public key) of an external *Certification Authority* (CA) you trust. That way, all incoming e-mails whose certificates were signed by this CA will be trusted, too. If you have selected the *Automatic Extraction of S/MIME Certificates* option on the *Mail Security >> Encryption >> Options* tab, certificates signed by a CA listed here will be extracted automatically and placed on the *Mail Security >> Encryption >> S/MIME Certificates* tab.

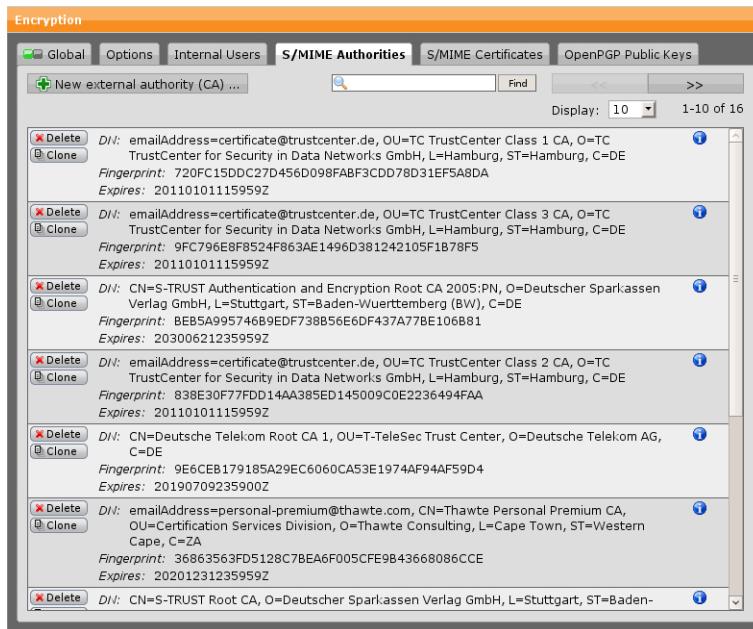


Figure 11.24 S/MIME Authorities List

To import an external S-MIME Authority, proceed as follows:

1. **On the S-MIME Authorities tab, click New External Authority (CA).**
The Add External Authority dialog box opens.
2. **Make the following settings:**
Format: Select the format of the CA. You can choose between the following formats:

- **der** (binary)
 - **pem** (ASCII)
-

Note – Microsoft Windows operating systems use the **.cer** file extension for both **der** and **pem** formats. You must therefore determine in advance whether the certificate you are about to upload is in binary or ASCII format. Then select the format from the drop-down list accordingly.

Certificate: Click on the folder icon to open the *Upload File* dialog box. Select the file and click *Save*.

Comment (optional): Add a description or other information about the external authority.

3. Click **Save**.

The CA appears on the *S/MIME Authorities* list.

Astaro Security Gateway ships with several public keys of commercial *Certification Authorities* (CA) pre-installed to facilitate e-mail encryption between your company and your communication partners who maintain a public key infrastructure (PKI) based on those CAs. The following links point to URLs of notable root certificates:

- Trustcenter³⁰
- S-TRUST³¹
- Thawte³²
- VeriSign³³
- GeoTrust³⁴

In addition, you can install the CA of another Astaro Security Gateway unit, thus enabling transparent e-mail encryption between two Astaro Security Gateway units.

³⁰ http://www.trustcenter.de/root_certificates.htm

³¹ <http://www.s-trust.de/download/ausstellerzertifikate/index.htm>

³² <http://www.thawte.com/roots/>

³³ <http://www.verisign.com/support/roots.html>

³⁴ http://www.geotrust.com/resources/root_certificates/index.asp

S-MIME Certificates

On the *Encryption >> S/MIME Certificates* tab, you can import external S/MIME certificates. E-mails for recipients whose certificates are listed here will automatically be encrypted. If you want to disable encryption for a particular recipient, simply delete its certificate from the list.

Note – When you upload an S/MIME certificate manually, messages from the e-mail address associated with the certificate are always trusted, although no CA certificate is available that may identify the person noted in the certificate. That is to say, manually uploading an S/MIME certificate labels the source as trusted.

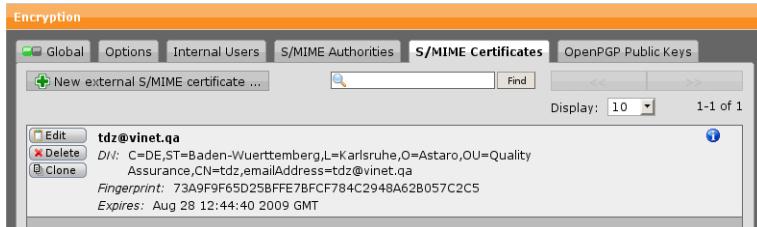


Figure 11.25 S/MIME Certificates List

To import an external S/MIME certificate, proceed as follows:

1. On the **S/MIME Certificates** tab, click **New External S/MIME Certificate**. The *Add S/MIME Certificate* dialog box opens.

2. Make the following settings:

Format: Select the format of the certificate. You can choose between the following formats:

- `pem` (ASCII)
- `der` (binary)

Note – Microsoft Windows operating systems use the `cer` file extension for both `der` and `pem` formats. You must therefore determine in advance whether the certificate you are about to upload is in binary or ASCII format. Then select the format from the drop-down list accordingly.

Certificate: Click on the folder icon to open the *Upload File* dialog box. Select the file and click *Save*.

Comment (optional): Add a description or other information about the certificate.

3. Click Save.

The new S/MIME certificate appears on the *S/MIME Certificates* list.

OpenPGP Public Keys

On the *Encryption >> OpenPGP Public Keys* tab you can install OpenPGP public keys. Files must be provided in .asc format. The upload of entire keyrings is supported.

Note – Do not upload a keyring that is protected by a passphrase.

All public keys included in the keyring will be imported and can be used to encrypt messages. E-mails for recipients whose public keys are listed here will automatically be encrypted. If you want to disable encryption for a particular recipient, simply delete its public key from the list.

Note – Only one e-mail address per key is supported. If there are multiple addresses attached to a key, only the "first" one will be used (the order may depend on how OpenPGP sorts addresses). If the key you want to import has several addresses attached, you must remove the unneeded addresses with OpenPGP or other tools prior to importing the key into Astaro Security Gateway.



Figure 11.26 OpenPGP Public Keys List

To import an OpenPGP public key, proceed as follows:

1. On the OpenPGP Public Keys tab, click Import Keyring File.

The Import OpenPGP Keyring File dialog box opens.

2. Upload the OpenPGP key(s).

Click on the folder icon to open the Upload file dialog box. Select the file and click Save.

The key or, if the file contains several keys, a list of keys is displayed.

3. Select one or more keys and click Import Selected Keys.

The key(s) appear(s) on the OpenPGP Public Keys list.

Note – An e-mail address must be attached to the key. Otherwise the installation will fail.

Quarantine Report

Astaro Security Gateway features an e-mail quarantine containing all messages (SMTP and POP3) that have been blocked and redirected to the quarantine for various reasons. This includes messages waiting for delivery as well as messages that are infected by malicious software, contain suspicious attachments, are identified as spam, or simply contain unwanted expressions.

Time	From	To	Subject	Reason	Size	Action
Jul 21 05:21:47	fh405@*****	*****	You've Won	Spam	1KB	Release Whitelist
Jul 21 04:10:15	meghann.petrucci@*****	*****	You've Won	Spam	1KB	Release Whitelist
Jul 21 09:55:44	news@sktuell*****	*****	Verfalls heute, 24 Uhr: Nur 69,95 EUR statt 404,85 EUR: 500 GB extreme Festplatte + 10 Software-Vollversionen! Receipt for Your Payment to Digital River GmbH	Spam	56KB	Release Whitelist
Jul 21 14:17:19	payment@*****	*****	Philips Telefon für 24,99 Euro - der beste Preis im Internet!	Malware	14KB	
Jul 21 13:46:53	root@152.81.226.*****	*****		Spam	44KB	Release Whitelist
Jul 21 14:02:09	newsletter@*****	*****	5 Euro-Gutschein bei Shop-Apotheke, 15% Rabatt bei Brille24.de und viele weitere Top-Sommerangebote	Spam	50KB	Release Whitelist
Jul 21 14:04:32	news@*****	*****	Geschenkt! Prepaid-Handy inkl. 5,- EUR Startguthaben jetzt für 0,00 EUR statt 39,90 EUR!	Spam	57KB	Release Whitelist

Online Help:

To move an e-mail to your inbox, click its [Release](#) link.
 Alternatively, if you click the [Whitelist](#) link, the e-mail will be moved to your inbox and the sender of the e-mail is whitelisted for the future, that is, mail from this e-mail address will always be allowed.
 Note that you may only be able to release (and whitelist) messages with specific quarantine reasons. Please contact your system administrator if you require assistance.

To minimize the risk of messages being withheld that were quarantined mistakenly (so-called *false positives*), Astaro Security Gateway sends a daily Quarantine Report to the users informing them of messages in their quarantine. If users have several e-mail addresses configured, they will get an individual Quarantine Report for each e-mail address. This also applies if a user has additional POP3 accounts configured in his User Portal, provided the POP3 proxy of Astaro Security Gateway is in *prefetch* mode, which allows the prefetching of messages from a POP3 server and storing them in a local database. In a Quarantine Report a user can click on any spam entry to release the message from the quarantine or to whitelist the sender for the future.

The following list contains some more information about the Quarantine Report:

- Quarantine Reports are only sent to those users whose e-mail address is part of a domain contained in any SMTP profile. This includes the specification in the *Domains* box on the *SMTP >> Routing* tab as well as the specifications in the *Domains* box of any SMTP Profile.
- If the POP3 *prefetch* option is disabled, quarantined messages sent to this account will not appear in the Quarantine Report. Instead, each user will find the typical Astaro POP3 blocked message in his inbox. It is therefore not possible to release the message by means of the Quarantine Report or the User Portal. The only way to deliver such an e-mail is to download it in *zip* format from the Mail Manager by the administrator.
- Only spam e-mails can be released from the quarantine. Messages quarantined for other reasons, for example because they contain viruses or suspicious file attachments, can only be released from the quarantine by the administrator in the Mail Manager of Astaro Security Gateway. In addition, users can also review all of their messages currently held in quarantine in the Astaro User Portal.
- If a spam e-mail has multiple recipients, as is the case with mailing lists, when any one recipient releases the e-mail, it is released for that recipient only, provided the e-mail address of the mailing list is configured on the system. Otherwise the e-mail will be sent to all recipients simultaneously. For more information, see the *Define internal mailing lists* option on the *Mail Security >> Quarantine Report >> Exceptions* tab.
- E-mails sent to an SMTP e-mail address for which no user is configured in Astaro Security Gateway can be released (but not whitelisted) from the

Quarantine Report or in the Mail Manager by the administrator. However, as this user is not configured, no access to the User Portal is possible.

- Spam e-mails sent to mailing lists cannot be whitelisted.
- Some e-mail clients do not encode the header of an e-mail correctly, which may result in an awkward representation of the e-mail in the daily Quarantine Report.

Global

On the *Quarantine Report >> Global* tab you can define at what time the daily Quarantine Report shall be sent and write a message text that will appear in the Quarantine Reports.

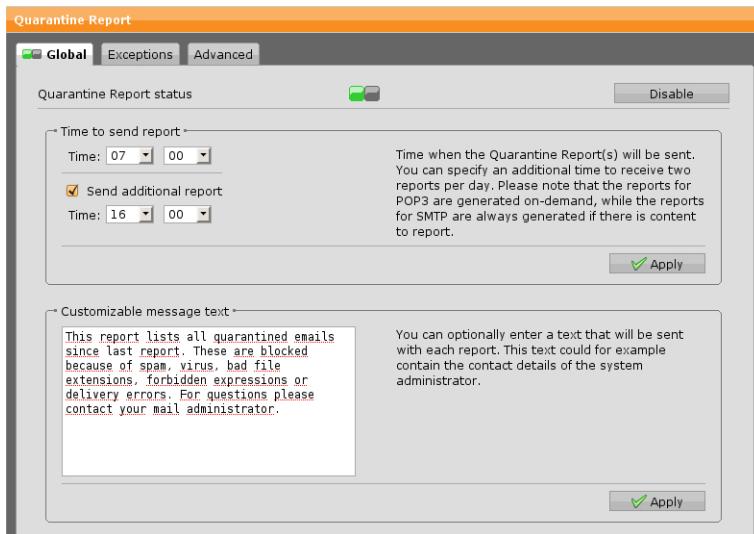


Figure 11.28 Quarantine Report Global Settings

To edit the Quarantine Report settings, enable the Quarantine Report: You can either click the status icon or the *Enable* button.

The status icon turns green.

Time to Send Report

Here you can define when the daily Quarantine Report(s) will be sent. Select the time using the drop-down lists and click *Apply*.

You can also send an additional report. For this, select the checkbox *Send Additional Report*, set the time, and click *Apply*.

Customizable Message Text

Here you can customize the text which forms the introduction of the Quarantine Report. Change the message text according to your needs and click **Apply**.

Note – It is not possible to use HTML tags in the customizable message text box.

Note – Customization is not possible when using a home use license.

Exceptions

On the *Quarantine Report >> Exception* tab you can define a skip list of e-mail addresses that should be exempt from receiving daily Quarantine Reports.

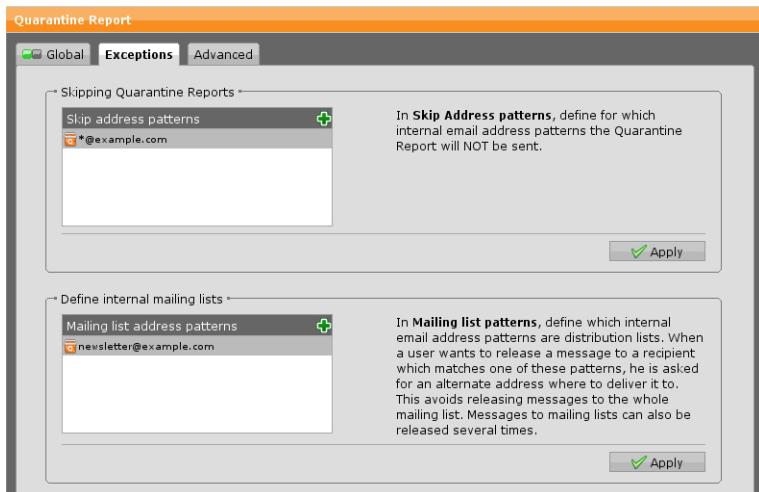


Figure 11.29 Quarantine Report Exceptions

Skiping Quarantine Reports

Here you can configure internal e-mail addresses for which no quarantine notifications should be sent. Users whose e-mail addresses are listed here will not receive daily Quarantine Reports. You can enter full e-mail addresses or use an asterisk (*) as wildcard, for example *@example.com.

Note – The skip list only applies for the SMTP Quarantine Report. If there is a POP3 account specified for the respective user, the POP3 Quarantine Report will be sent nonetheless.

Define Internal Mailing Lists

If the e-mail address of a mailing list is configured in the *Mailing List Address Patterns* box (e.g., newsletter@example.com) and a spam message sent to this mailing list was detected and redirected to the e-mail quarantine, the Quarantine Report of all recipients included in this mailing list will contain a link to this spam message. Thus, each recipient can release this spam message individually by entering his e-mail address in a user prompt that appears once the recipient has clicked the *Release* link in the Quarantine Report.

Note – Mailing lists cannot be whitelisted in the Quarantine Report or the User Portal.

Alternatively, you could enter the e-mail address of that particular mailing list as an additional e-mail address in a local user's profile; this user becoming some sort of a mail manager. Then only this user's Quarantine Report will contain a link to the spam message that was sent to the mailing list. Clicking the *Release* link will deliver the spam message to all recipients of that mailing list at once.

Note – If the e-mail address of a mailing list is configured as an additional e-mail address in a user's profile, no recipient included in that mailing list gets displayed the links to spam messages that were sent to this mailing list.

However, if the e-mail address of a mailing list is both configured as an additional e-mail address in a user's profile and in the *Mailing List Address Patterns* box, then the *Release* link in that user's Quarantine Report will open a user prompt. The user is then to decide who is going to receive the spam mail by manually entering the respective e-mail addressee(s) to forward the spam message to.

Finally, if the e-mail address of a mailing list is neither configured as an additional e-mail address in a user's profile nor as a mailing list address pattern, a spam message sent to the mailing list is handled like a normal e-mail, meaning

that if any one recipient releases the spam mail, it will be sent to all recipients of the mailing list.

To sum up, whenever the e-mail address of a mailing list is configured as a mailing list address pattern, each user having a link to the spam message in his Quarantine Report is prompted to enter an e-mail address to release the spam message to.

Advanced

In the *Quarantine Report >> Advanced* tab you can configure an alternative hostname and port number for the Release links contained in daily Quarantine Reports. Additionally, you can change the release options for spam e-mails.

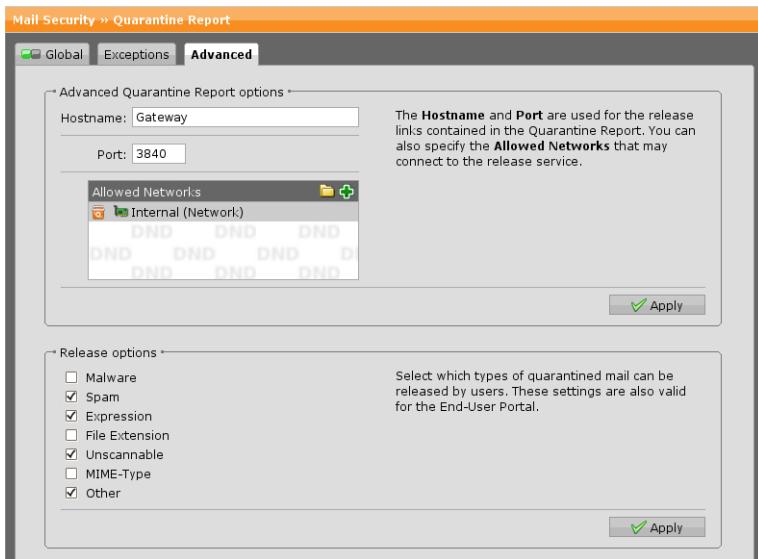


Figure 11.30 Advanced Quarantine Report Options

Advanced Quarantine Report Options

Hostname: By default, this is the firewall's hostname as given in the *Mail Security >> SMTP >> Advanced Settings* area. However, it is possible to specify an alternative portal hostname. By default, these links point to the hostname of the firewall. However, if you want to enable users to release their e-mails across the Internet, it might be useful to enter an alternative hostname here that can be resolved publicly.

Port: By default, port 3840 is configured. You can change the port to any value

in the range from 1024 to 65535.

Allowed Networks: You can also specify the networks that should be allowed to connect to the e-mail release service. By default, only the internal network is selected.

Click *Apply* to save your settings.

Release Options

Here you can select which types of quarantined messages shall be releasable by users. You can choose between the following options:

- Malware
- Spam
- Expression
- File Extension
- Unscannable
- MIME Type
- Other

Click *Apply* to save your settings.

Mail Manager

The Mail Manager is an administrative tool to manage and organize all e-mail messages currently stored on the unit. This includes messages waiting for delivery as well as quarantined messages that are infected by malicious software, contain suspicious attachments, are identified as spam, or contain unwanted expressions. You can use the Mail Manager to review all messages before downloading, releasing, or deleting them. The Mail Manager is fully UTF-8 capable.

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

The screenshot shows the Mail Manager window with the "SMTP Quarantine" tab selected. At the top, there are five tabs: "SMTP Quarantine", "SMTP Spool", "SMTP Log", "POP3 Quarantine", and "Close". Below the tabs are two rows of filter options. The first row, "Result Filter", includes checkboxes for "Delivered", "Rejected", "Quarantined", "Blackholed", "Cancelled", "Bounced", "Deleted", and "Unknown". The second row, "Reason Filter", includes checkboxes for "Malware", "Span", "Expression", "File Extension", "MIME Type", "Unscannable", "Rpt verification", and "SPF". There are dropdown menus for "Profile/Domain" (set to "All") and "IP/NetAddress/Subj. substring" (empty), and a "Received date:" field with a calendar icon. The main content area displays a list of 39 events matching the filter settings, sorted by event time, newest first. Each entry includes a small thumbnail, the date and time, the IP address, the number of attachments, the file extension, and the reason for quarantine. For example, the first entry is from 2008-08-15 12:17, IP 10.8.2.198, 11 attachments, file.qsa, and the reason is "Delivered > 10.0.3.13 (10.0.3.13)". The list continues with other entries for various dates, IP addresses, attachment counts, file extensions, and reasons like "Quarantined: Malware (EICAR_Test_File (exact))".

Figure 11.31 Mail Manager of Astaro Security Gateway

Mail Manager Window

To open the Mail Manager window click the button *Open Mail Manager in New Window* on the *Mail Security >> Mail Manager >> Global* tab. The Mail Manager is divided into five different tabs:

- **SMTP Quarantine:** Displays all messages that are currently quarantined.
- **SMTP Spool:** Displays all messages currently in /var/spool. This may be due to them waiting for delivery or because of an error.
- **SMTP Log:** Displays the delivery log for all messages processed via SMTP.
- **POP3 Quarantine:** Displays all messages fetched via POP3 that are currently quarantined.
- **Close:** Click here to close the Mail Manager window.

SMTP/POP3 Quarantine

Messages in SMTP and POP3 Quarantine can be displayed according to their respective quarantine cause:

- Malware
- Spam

- Expression
- File Extension
- MIME Type (SMTP only)
- Unscannable
- Other

Use the checkboxes to select/unselect quarantine causes. Double-click the checkbox of a cause to solely select this cause.

Hint – Double-click a message to view it.

Profile/Domain (SMTP), Accounts (POP3): Select a profile/domain or account to show its messages only.

Sender/Rcpt/Subject Substring: Here you can enter a sender, recipient or subject to search for in the quarantined messages.

Received Date: To only show messages processed during a certain time frame, enter a date or select a date from the calendar icon.

Sort By: Messages can be sorted by date, subject line, sender address, and message size.

And Show: You can choose between displaying 20, 50, and 100 entries per page and all messages. Note that showing all messages may take a lot of time.

Use the checkbox in front of each message or click a message to select it to apply actions on the selected messages. The following actions are available:

- **Download:** Selected messages will be downloaded.
- **Delete:** Selected messages will be deleted irrevocably.
- **Release:** Selected messages will be released from quarantine.
- **Release and Report as False Positive:** Selected messages will be released from quarantine and reported as false positive to the spam scan engine.

Note that only the administrator can release *all* messages held in quarantine. Users reviewing their messages in the Astaro User Portal can only release messages they are explicitly allowed to. The authorization settings for this can be found on the *Mail Security >> Quarantine Report >> Advanced* tab.

Select Global Cleanup Action: Here you find several deletion options that will be applied on messages globally, that is, regardless whether they are selected and/or displayed or not.

Caution – Deleted messages are irrevocable.

SMTP Spool

Here you see messages that are either waiting for delivery or have produced an error. The delivery log is also part of the message header. Use the following checkboxes to select only one type of messages for display:

- **Waiting:** Messages waiting for delivery.
- **Error:** Messages that caused an error. If a messages produces an error more than once, please report the case to your Astaro Partner or the Astaro Support Team.

Hint – Double-click a message to view it.

Profile/Domain: Select a profile/domain to show its messages only.

Sender/Rcpt/Subject Substring: Here you can enter a sender, recipient, or subject to search for in the spool messages.

Received Date: To only show messages processed during a certain time frame, enter a date, or select a date from the calendar icon.

Sort By: Messages can be sorted by date, sender address, subject line, and message size.

And Show: You can choose between displaying 20, 50, 100, 250, 500, and 1000 entries per page and all messages. Note that showing all messages may take a lot of time.

Use the checkbox in front of each message or click a message to select it to apply actions on the selected messages. The following actions are available:

- **Download:** Selected messages will be downloaded.
- **Retry:** For selected messages delivery will be retried immediately.

- **Delete:** Selected messages will be deleted irrevocably.
- **Bounce:** Selected messages will be bounced, that is the sender will receive a message that the delivery of their message has been cancelled.

Select Global Cleanup Action: Here you find a retry option and several deletion options that will be applied on messages globally, that is, regardless whether they are selected and/or displayed or not.

Caution – Deleted messages are irrevocable.

SMTP Log

The *SMTP Log* displays the log messages for all messages processed via SMTP. **Result Filter:** Select which type of message will be displayed by selecting the corresponding checkboxes.

- **Delivered:** Successfully delivered messages.
- **Rejected:** Messages rejected by the ASG.
- **Quarantined:** Quarantined messages.
- **Blackholed:** Messages that have been deleted without notification.
- **Cancelled:** Messages that have been manually bounced in *SMTP Spool*.
- **Bounced:** Messages that could not be delivered, for example because of false routing settings.
- **Deleted:** Messages that have been manually deleted.
- **Unknown:** Messages whose status is unknown.

Use the checkboxes to select/unselect *Result Filter* items. Double-click an item to solely select this item.

Reason Filter: Use the checkboxes to further filter the message log display.

Hint – Double-click a message log to view it. Click on the server icon of a message to resolve the IP address. An asterisk (*) denotes a successful reverse DNS lookup.

Profile/Domain: Select a profile/domain to show its messages only.

IP/Net/Address/Subj. Substring: Here you can enter an IP address, network address, or subject to search for in the SMTP log messages.

Received Date: To only show messages processed during a certain time frame, enter a date, or select a date from the calendar icon.

Sort By: Messages can be sorted by event time, sender address, and message size.

And Show: You can choose between displaying 20, 50, and 100 entries per page and all messages. Note that showing all messages may take a lot of time.

Global

In the upper part of the *Mail Manager >> Global* tab you can open the Mail Manager by clicking the *Open Mail Manager in New Window* button.

The screenshot shows the 'Mail Security >> Mail Manager' interface with the 'Global' tab selected. The main area displays a 'Statistics Overview' table comparing SMTP and POP3 stored messages. The table includes sections for 'Waiting for delivery (spooled)', 'Quarantined items', and 'Quarantined totals' for both protocols. Below this, a section titled 'SMTP last 24 hours' provides a summary of recent activity, including counts for malware, spam, and various reject types.

Statistics Overview			
SMTP stored messages		POP3 stored messages	
Waiting for delivery (spooled):	0	Waiting for client pickup:	0
Quarantined malware:	5	Quarantined malware:	3
Quarantined spam:	5	Quarantined spam:	10
Quarantined expression:	2	Quarantined expression:	1
Quarantined file extension:	0	Quarantined file extension:	2
Quarantined unscannable:	2	Quarantined unscannable:	1
Quarantined MIME-Type:	2		
Quarantined total:	16	Quarantined total:	17
SMTP last 24 hours [3 messages delivered, 36 messages blocked (92%)]			
Malware quarantined/rejected:	5	SPF rejects:	0
Spam quarantined/rejected:	10	RBL rejects:	0
Blacklist rejects:	0	BATV rejects:	0
Address Verification rejects:	0	RDNS/HELO rejects:	15

Figure 11.32 Mail Manager: Overview

In the lower part, the *Statistics Overview* area provides an overview of all messages currently stored on the unit. Data is divided into messages that were

delivered via the SMTP or POP3 protocol. For both types, the following information is displayed:

- **Waiting for Delivery (Spooled)** (SMTP only): Mails that are currently in spool, for example because they were being scanned and could not be delivered yet.
- **Waiting for Client Pickup** (POP3 only): Mails that have been prefetched by the unit and have not yet been collected by a client/user.
- **Quarantined Malware**: The total of messages that contain malware, such as viruses or other harmful content.
- **Quarantined Spam**: The total of messages that were identified as spam.
- **Quarantined Expression**: The total of messages that were diverted to the quarantine because they contain forbidden expressions.
- **Quarantined File Extension**: The total of messages held in quarantine because they contain suspicious attachments (identified by their file extension).
- **Quarantined Unscannable**: The total of messages held in quarantine because it could not be scanned.
- **Quarantined MIME Type** (SMTP only): The total of messages held in quarantine because they contain MIME types that are to be filtered according to the SMTP settings.
- **Quarantined Total**: The total of messages that are held in quarantine.

Note – The numbers for *Waiting for Delivery* represent a real-time snapshot for SMTP messages. However, for POP3 messages, the numbers presented are the accumulation of data since the last time prefetching was enabled.

Below you see a short statistic for SMTP quarantining and rejections of the last 24 hours:

- **Malware Quarantined/Rejected**: Messages quarantined/rejected because they contain harmful content.
- **Spam Quarantined/Rejected**: Messages quarantined/rejected because they have been identified as spam.

- **Blacklist Rejects:** Messages rejected because the sender is on a blacklist.
- **Address Verification Rejects:** Messages rejected because the sender address could not be verified.
- **SPF Rejects:** Messages rejected because sending host is not allowed.
- **RBL Rejects:** Messages rejected because the sender is on a realtime black-hole list.
- **BATV Rejects:** Messages rejected because BATV tag could not be validated.
- **RDNS/HELO Rejects:** Messages rejected due to invalid HELO or missing RDNS entries.

Whether there are any rejects depends on your settings in *Mail Security >> SMTP*.

Configuration

On the *Mail Manager >> Configuration* tab you can configure how long the database log will be kept and after how many days quarantined messages are to be deleted from the quarantine. Any logs and messages that are older than the number of days in the expiration settings will be deleted automatically.

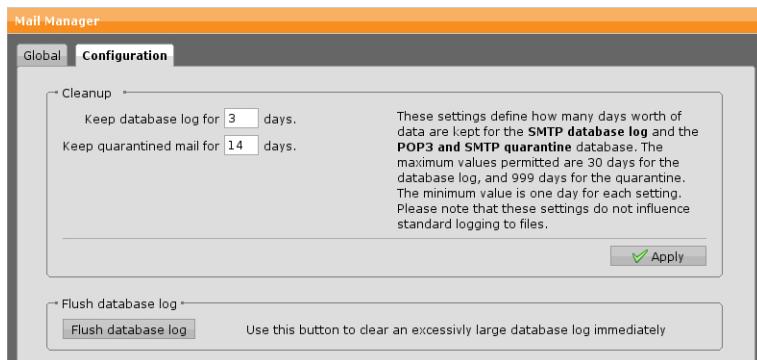


Figure 11.33 Configuration of Mail Manager

The default settings are as follows:

- Database log will be deleted after three days. Maximum number permitted: 30 days.
- Quarantined messages will be deleted after 14 days. Maximum number permitted: 999 days.

The minimum number of days permitted for both database log and quarantine is one day.

Flush Database Log

This option is useful if your database log has accumulated an immense amount of data to clear the log immediately. That way you do not have to wait for the normal cleanup action to apply.

RED Management

This chapter describes how to configure Astaro RED. RED is short for *Remote Ethernet Device* and is a means to connect remote branch offices and the like to your main office as if the branch office is part of your local network.

The setup consists of the Astaro Security Gateway in your main office and a Remote Ethernet Device (RED) in your remote office. Establishing a connection between the two is utmost easy as the RED appliance itself does not need to be configured at all. As soon as the RED appliance is connected to your ASG it behaves like any other Ethernet device on your ASG. All traffic of your branch office is safely routed via your ASG which means that your branch office is as secure as your local network.

The following topics are included in this chapter:

- Global Settings
- Device Configuration
- What is RED?

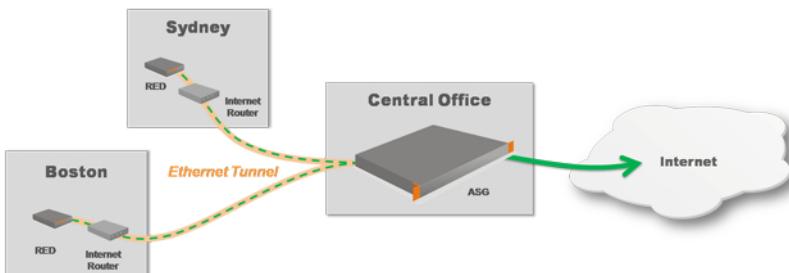


Figure 12.1 RED: Setup Sketch

Setting up a RED environment involves the following steps:

1. Activation of RED support.
2. Configuration of the RED appliance on your ASG.
3. Connecting the RED appliance to the Internet on the remote site.

Note – The overview page of RED displays general information on the RED architecture as long as no RED appliance is configured. When a RED appliance has been configured, the page will display information on the RED status.



Figure 12.2 RED: Site Status on the Overview Page

Open RED Live Log

You can use the live log to monitor the connection between your Astaro Security Gateway and the RED appliance. Click the *Open RED Live Log* button to open the live log in a new window.

Global Settings

On the *Global Settings* tab you can enable or disable the support for RED which means that your ASG acts as a RED hub. You need to enable the RED support before any RED appliances can connect to the ASG.

To enable RED support, do the following:

1. On the *Global Settings* tab, enable RED support.

You can either click the status icon or the *Enable* button.

The status icon turns amber and the RED Hub Configuration becomes editable.

2. Enter your organization details.

By default the settings from the *Management >> System Settings >> Organizational* tab is used.

3. Click *Activate RED*.

The status icon turns green and RED support is activated. Your ASG is now registered at the RED Provisioning Service (RPS) of Astaro to act as a RED

hub.

You can now continue by adding one or more RED appliances on the *RED >> Device Configuration* page.

To cancel the configuration, click *Abort Enable* or the amber colored status icon.

Device Configuration

On the *Device Configuration* page you can configure your Remote Ethernet Device (RED) appliances. Each appliance that is configured here is able to establish a connection to your ASG.

Note – For RED appliances to be able to connect, you need to enable RED support on the *Global Settings* page first.

To add a RED appliance, do the following:

1. On the *Device Configuration* tab, click *Add RED Appliance*.

The *Add RED Appliance* dialog box opens.

2. Make the following settings:

Branch Name: Enter the name of the RED appliance branch, e.g. "Office Munich".

RED ID: Enter the ID of the RED appliance you are configuring. This ID can be found on the back of the RED appliance and on its packaging.

ASG Hostname: If this field is displayed below *RED ID*, the IP of your ASG is either not publicly resolvable and/or uses a private IP address. You need to enter a public IP address or hostname where the ASG is accessible.

Quick Remote Network Setup (optional): This option is selected by default. It helps you by automatically configuring basic network settings that are necessary for the RED appliance and your ASG to interact smoothly. In detail, the following configurations are made:

- The Ethernet object for the RED appliance is created, bearing the name *reds* followed by a number, e.g. "reds1".
- The network interface and the network definitions are created, both of which bearing the name given in the *Branch Name* field.

- The RED appliance is added to the DNS Allowed Networks (*Network Services >> DNS >> Global*).
- For the given IP range, a DHCP server is created which provides IP addresses to the appliances of the remote site, using the IP address range .100–.254.

If you disable the *Quick Remote Network Setup* option, you need to do these four configurations manually.

Note – You always have to make the following configurations manually:
1) Creating the necessary packet filter rules (*Network Security >> Packet Filter >> Rules*). 2) Creating the necessary masquerading rules (*Network Security >> NAT >> Masquerading*).

Base (ASG) IP: Provide the first IP address of the IP address range that the remote site, where the RED appliance resides, is to be used. The RED Ethernet object itself always uses the IP address ending with .1, e.g. 192.168.200.1. This means that you cannot provide an IP address here other than ending with .1. Note that, as the RED appliance behaves like any other Ethernet device of your ASG, you can change its settings on the *Definitions >> Networks* tab.

Advanced (optional): You only need to fill in the fields of this section if the RED appliance you are configuring has been used by another ASG before. It is then necessary to provide its unlock code—otherwise the RED appliance is not going to interact with the actual ASG.

Unlock Code: Provide the unlock code of the RED appliance you are configuring. If you are not in the possession of the unlock code, the only way to unlock the RED appliance is to contact the Astaro Support.

ASG Hostname: If this field is displayed under *Advanced*, it contains by default the IP address or hostname of the ASG that could be retrieved automatically. You can enter another IP address or hostname which must, however, be publicly resolvable.

3. Click **Save**.

The RED appliance is being created and the ASG registers with the Astaro RED Provisioning Service (RPS).

Important Note – It is crucial that you keep the *Unlock Code* which is e-mailed instantly to the address provided on the *Global* tab (during activation of RED) as soon as the RED appliance registers with the RPS. You need the unlock code when you want to use the RED appliance with another ASG. If you then do not have the unlock code ready, the only way to unlock the RED appliance is to contact the Astaro Support.

The RED appliance on the remote site can now be connected to the Internet. As soon as it has booted, it will fetch its configuration at the Astaro RED Provisioning Service (RPS). After that the connection between your ASG and the RED appliance is going to be established. You can see the appliance status of all configured RED appliances on the *RED* overview page of WebAdmin.

Deleting a RED appliance

To delete a RED appliance, click the *Delete* button next to the appliance name. There will be a warning that the RED object has dependencies. Be aware that deleting a RED appliance will *not* delete associated interfaces and their dependencies. This is intentional, since it enables you to move an interface from one RED appliance to another. Simply add the new RED appliance without using the *Quick Remote Network Setup* option, then assign the new RED hardware object to the existing interface definition.

If you want to remove a RED appliance setup completely, you need to delete potential interface and other definitions manually.

What is RED?

The page *What is RED?* provides general information on what RED is meant for, how it works, and how a typical RED setup looks like.

VoIP Security

Voice over Internet Protocol (VoIP) is the routing of voice conversations over the Internet or through any other IP-based network. Astaro Security Gateway offers support for the most frequently employed protocols used to carry voice signals over the IP network:

- SIP
- H.323

The *VoIP Security* statistics page in WebAdmin shows the number of SIP and H.323 connections for various time periods.

SIP

The *Session Initiation Protocol* (SIP) is a signalization protocol for the setup, modification, and termination of sessions between two or several communication partners. It is primarily used in setting up and tearing down voice or video calls. SIP uses TCP on port 5060 to negotiate which dynamic port range is to be used between the endpoints when setting up a call. Since opening all ports within the dynamic range would cause a severe security issue, the firewall is able to handle SIP traffic on an intelligent basis. This is achieved by means of a special connection tracking helper monitoring the control channel to determine which dynamic ports are being used and then only allowing these ports to pass traffic when the control channel is busy. For that purpose you must specify both a SIP server and a client network definition in order to create appropriate packet filter rules enabling the communication via the SIP protocol.

To enable support for the SIP protocol, proceed as follows:

1. On the *SIP* tab, enable SIP protocol support.

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *Global SIP Settings* area becomes editable.

2. Make the following settings:

SIP Server Networks: Here you can select the SIP server (provided by your ISP) the SIP clients should be allowed to connect to; for security reasons,



Figure 13.1 Configuring VoIP SIP Settings

do not select *Any*.

SIP Client Networks: Select the hosts/networks of the SIP clients that should be allowed to initiate or respond to a SIP communication. An SIP client is an endpoint that participates in real-time, two-way communications with another SIP client.

3. Click **Apply**.

Your settings will be saved.

To cancel the configuration, click *Abort* *Enable* or the amber colored status icon.

H.323

H.323 is an international multimedia communications protocol standard published by the *International Telecommunications Union* (ITU-T) and defines the protocols to provide audio-visual communication sessions on any packet-switched network. H.323 is commonly used in *Voice over IP* (VoIP) and IP-based videoconferencing.

H.323 uses TCP on port 1720 to negotiate which dynamic port range is to be used between the endpoints when setting up a call. Since opening all ports within the dynamic range would cause a severe security issue, the firewall is able to allow H.323-related traffic on an intelligent basis. This is achieved by means of a special connection tracking helper monitoring the control channel to determine which dynamic ports are being used and then only allowing these ports to pass traffic when the control channel is busy. For that purpose you must specify both an H.323 gatekeeper and a client network definition in order

to create appropriate packet filter rules enabling the communication via the H.323 protocol.

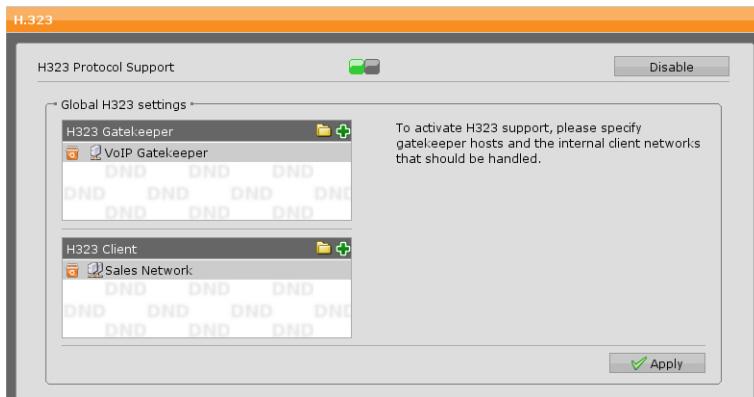


Figure 13.2 Configuring VoIP H.323 Settings

To configure support for the H.323 protocol, proceed as follows:

1. **On the *H.323* tab, enable H.323 protocol support.**

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *Global H.323 Settings* area becomes editable.

2. **Make the following settings:**

H.323 Gatekeeper: Select an H.323 gatekeeper. An H.323 gatekeeper controls all H.323 clients (endpoints such as Microsoft's NetMeeting) in its zone. More specifically, it acts as a monitor of all H.323 calls within its zone on the LAN. Its most important task is to translate between symbolic alias addresses and IP addresses.

H.323 Client: Here you can select the host/network to and from which H.323 connections are initiated. An H.323 client is an endpoint in the LAN that participates in real-time, two-way communications with another H.323 client.

3. **Click *Apply*.**

Your settings will be saved.

To cancel the configuration, click *Abort Enable* or the amber colored status icon.

Chapter 14

IM/P2P

This chapter describes how to configure *Instant Messaging* (IM) and *Peer-to-Peer* (P2P) security features of Astaro Security Gateway.

A dedicated sub-system to classify network traffic, called the *Astaro Flow Classifier* (AFC), is used to detect instant messaging and peer-to-peer protocols. Whenever a feature of the Astaro Security Gateway requires network traffic to be classified, the AFC sub-system becomes active. For the sub-system to work you need to activate IM/P2P control on the *Settings* tab and to set at least one protocol to a control status other than *Do not control*. AFC is only active for those protocols which are set to be controlled.

The *Instant Messaging/Peer-to-Peer Statistics* page in WebAdmin shows an overview of the most used IM and P2P protocols as well as the top source IP addresses using those services. Each of the sections contains a *Details* link. Clicking the link redirects you to the respective *Reporting* section of WebAdmin, where you can find more statistical information.

The following topics are included in this chapter:

- Settings
- Instant Messaging (IM)
- Peer-to-Peer (P2P)

Settings

The tabs under *IM/P2P >> Settings* affect everything related to network traffic classification with the *Astaro Flow Classifier* (AFC) sub-system.

Note – These settings really do affect all of the Astaro Flow Classifier, including the pre-defined "AFC" traffic selectors in *Network >> Quality of Service (QoS) >> Traffic Selectors*.

Global

On the *Settings >> Global* tab you can activate the *Astaro Flow Classifier* (AFC) sub-system.

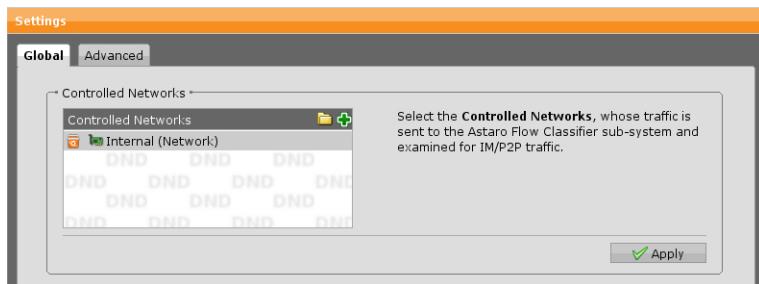


Figure 14.1 Configuring IM/P2P Global Settings

To configure IM/P2P, proceed as follows:

1. **Select the controlled networks:**

Select the networks that should be examined for IM/P2P traffic.

2. **Click *Apply*.**

Your settings will be saved.

Advanced

On the *Settings >> Advanced* tab you can exclude single hosts or networks from the IM/P2P controlled networks. Also, logging settings allow to control how verbose the Astaro Flow Classifier logs classified traffic.

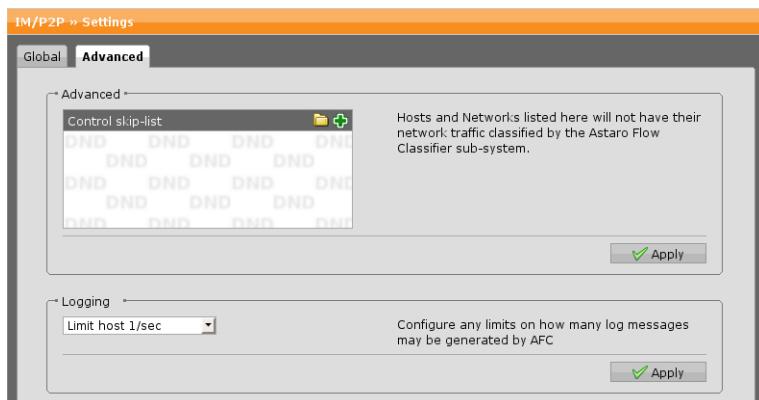


Figure 14.2 Configuring IM/P2P Advanced Settings

Advanced

Hosts and networks listed in the *Control Skip-List* are excluded from the

IM/P2P traffic control by the Astaro Flow Classifier, i.e. neither incoming nor outgoing traffic of these hosts or networks will be checked for IM/P2P patterns.

Logging

This option lets you select the log level to prevent certain IM/P2P clients from generating too many log entries with a large number of short-lived connections. The following levels are available:

- **Off:** Select this log level if you want to turn logging completely off.
- **Limit All 5/Sec:** Limit logging to five packets per second.
- **Limit Host 1/Sec:** Limit the number of log messages a single host can generate to one per second. This level is set as default.
- **Log All:** Select this log level if you want verbose logging for all IM/P2P traffic. Note that may lead to extensive logging.

Instant Messaging (IM)

Instant Messaging (IM) is a form of real-time communication between two or more communication partners based on typed text. Generally speaking, it requires the use of a client program that hooks up an instant messaging service and differs from e-mail in that conversations are able to happen in real-time.

Astaro Security Gateway has predefined a list of popular instant messaging services, letting you decide how to proceed with traffic that has been identified as instant messaging by the Astaro Flow Classifier sub-system.

Security Note – Network traffic classification is never as exact as, for example, controlling a specific TCP port. A certain level of ambiguity always remains: client protocols may change, or look very similar to innocuous traffic and thus prevent the use of simplistic classification algorithms. As such, IM/P2P control should be considered a tool to mitigate risk, protect resources and detect policy violations. It is not a technical solution that can replace more appropriate means to enforce a strict security policy.

Protocols

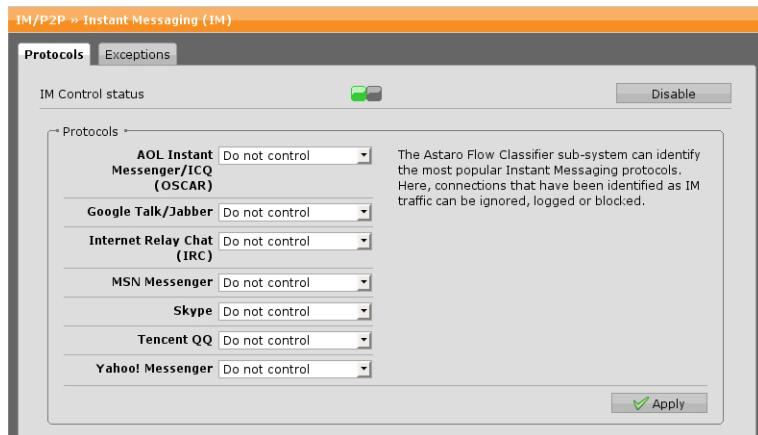


Figure 14.3 Configuring Instant Messaging Services

To edit the protocol settings enable the IM control. You can either click the status icon or the *Enable* button.

The status icon turns green and the *Protocols* area becomes editable. You can perform the following actions for each IM service:

- **Do Not Control:** Do not attempt to detect or restrict this instant messaging protocol. Instant messaging traffic can pass the firewall unrestricted.
- **Log:** The appropriate instant messaging traffic will be logged when passes the firewall.
- **Block File Transfers:** No files can be transferred between communication partners participating in a chat.

Note – For some protocols this option is currently not supported and therefore grayed out.

- **Block Completely:** No instant messaging traffic of this type can pass the firewall.

The following instant messaging services can be controlled:

- AOL Instant Messenger (AIM) and ICQ (OSCAR)
- Google Talk/Jabber

- Internet Relay Chat (IRC)
 - MSN Messenger
 - Skype
 - Tencent QQ
 - Yahoo! Messenger

Note – Skype connections may not be blocked reliably due to Skype's various efforts to obfuscate its traffic.

Exceptions

On the *Instant Messaging (IM) >> Exceptions* tab you can define more fine-grained exclusion from actions by the Astaro Flow Classifier. Unlike the *Control Skip-List* option on the *Settings >> Advanced* tab, exceptions are evaluated after the network traffic has been classified. This makes it possible, for example, to exclude a host or network from one specific protocol setting, while having all other settings still apply.

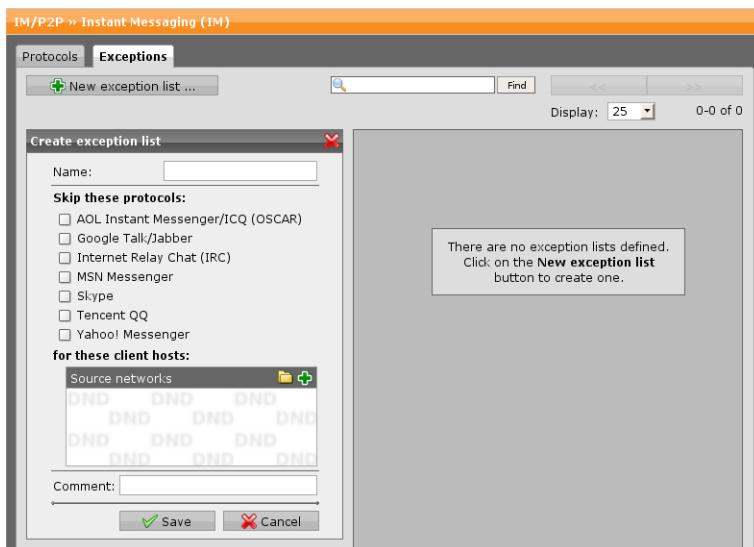


Figure 14.4 Instant Messaging Exceptions List

To create an exception, proceed as follows:

1. **On the *Exceptions* tab, click *New exception list*.**

The *Create Exception List* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for this exception.

Skip These Protocols: Select the instant messaging protocols that should be skipped.

For These Client Hosts: Select the source hosts/networks that should be exempt from the actions by the Astaro Flow Classifier of this exception rule.

Comment (optional): Add a description or other information about the exception.

3. **Click *Save*.**

The new exception appears on the *Exceptions* list.

To either edit or delete an exception list, click the corresponding buttons.

Peer-to-Peer (P2P)

A peer-to-peer (P2P) computer network is a network that relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a number of servers. A pure P2P network does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network. This particularity makes a P2P network useful for many purposes, most notably for file sharing, that is, the practice of making files available for other users to download over the Internet.

Astaro Security Gateway has predefined a list of popular P2P services, letting you decide how to proceed with each traffic that has been identified as peer-to-peer service by the Astaro Flow Classifier sub-system.

Security Note – Network traffic classification is never as exact as, for example, controlling a specific TCP port. A certain level of ambiguity always remains: client protocols may change, or look very similar to innocuous traffic and thus prevent the use of simplistic classification algorithms. As such, IM/P2P control should be considered a tool to mitigate risk, protect resources and detect policy violations. It is not a technical solution that can replace more appropriate means to enforce a strict security policy.

Protocols

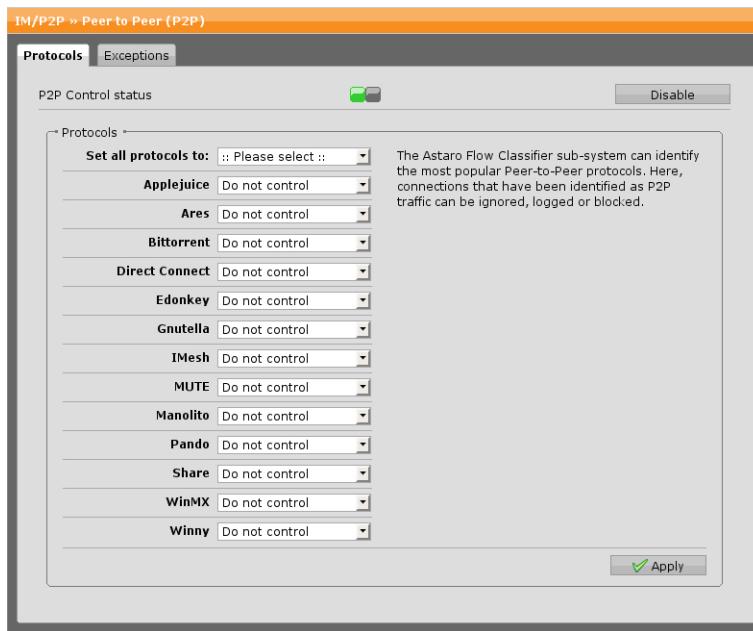


Figure 14.5 Configuring Peer-to-Peer Services

To edit the protocol settings enable the P2P control. You can either click the status icon or the *Enable* button.

The status icon turns green and the *Protocols* area becomes editable. You can perform the following actions for each P2P service:

- **Do Not Control:** Do not attempt to detect or restrict this peer-to-peer protocol. P2P traffic can pass the firewall unrestricted.
- **Log:** The appropriate P2P traffic will be logged when passing the firewall.
- **Block Completely:** No P2P traffic can pass the firewall.

It is however possible to centrally control all services by setting the field *Set all protocols to* to the desired value.

The following peer-to-peer services can be controlled individually:

- Applejuice
- Ares
- BitTorrent
- Direct Connect
- Edonkey
- Gnutella
- IMesh
- MUTE
- Manolito
- Pando
- Share
- WinMX
- Winny

Exceptions

On the *Peer-to-Peer (P2P) >> Exceptions* tab you can define more fine-grained exclusion from actions by the Astaro Flow Classifier. Unlike the *Control Skip-List* option on the *Settings >> Advanced* tab, exceptions are evaluated after the network traffic has been classified. This makes it possible, for example, to exclude a host or network from one specific protocol setting, while having all other settings still apply.

To create an exception, proceed as follows:

1. **On the *Exceptions* tab, click *New exception list*.**

The *Create Exception List* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for this exception.

Skip These Protocols: Select the Peer-to-Peer protocols that should be skipped.

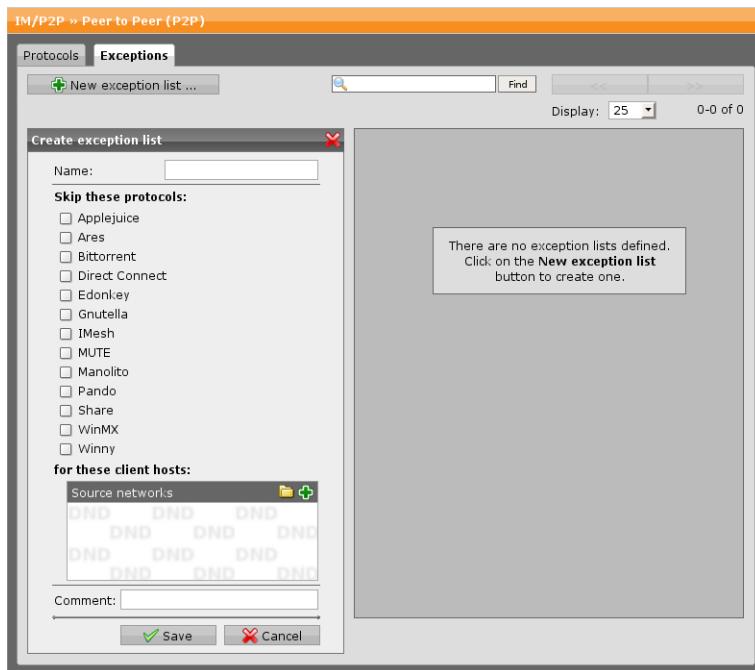


Figure 14.6 Peer-to-Peer Exceptions List

For These Client Hosts: Select the source hosts/networks that are to be exempt from the actions by the Astaro Flow Classifier of this exception rule.
Comment (optional): Add a description or other information about the exception.

3. Click Save.

The new exception appears on the *Exceptions* list.

To either edit or delete an exception list, click the corresponding buttons.

Site-to-site VPN

This chapter describes how to configure site-to-site VPN settings of Astaro Security Gateway. Site-to-site VPNs in Astaro Security Gateway are realized by means of *Virtual Private Networks* (VPNs), which are a cost effective and secure way for remote networks to communicate confidentially with each other over a public network such as the Internet. They use the cryptographic tunneling protocol IPSec to provide confidentiality and privacy of the data transmitted over them.

Cross Reference – Detailed information on how to configure site-to-site VPN connections can be found in the Astaro knowledgebase³⁵ (navigate to *ASG Version 7 >> Astaro Manuals and Guides*).

The following topics are included in this chapter:

- IPSec
- SSL
- Certificate Management

The *Site-to-site VPN* overview page in WebAdmin shows all configured IPSec and SSL connections and their current status. The state of each connection is reported by the color of its status icons. There are two types of status icons. The larger ones next to the connection name inform about the overall status of a connection. The different colors mean:

- Green – All SAs (*Security Association*) have been established. Connection is fully functional.
- Yellow – Not all SAs have been established. Connection is partly functional.
- Red – No SAs have been established. Connection is not functional.

The smaller ones next to the tunnel information report the status for that tunnel. Here the colors mean:

³⁵ <http://www.astaro.com/kb/>

- Green – All SAs have been established. Tunnel is fully functional.
- Yellow – IPSec SA has been established, ISAKMP SA (*Internet Security Association and Key Management Protocol*) is down. Tunnel is fully functional.
- Red – No SAs have been established. Connection is not functional.

IPSec

IP Security (IPSec) is a standard for securing *Internet Protocol* (IP) communications by encrypting and/or authenticating all IP packets.

The IPSec standard defines two service modes and two protocols:

- Transport mode
- Tunnel mode
- *Authentication Header* (AH) authentication protocol
- *Encapsulated Security Payload* (ESP) encryption (and authentication) protocol

IPSec also offers methods for manual and automatic management of *Security Associations* (SAs) as well as key distribution. These characteristics are consolidated in a *Domain of Interpretation* (DOI).

IPSec Modes

IPSec can work in either transport mode or tunnel mode. In principle, a host-to-host connection can use either mode. If, however, one of the endpoints is a security gateway, the tunnel mode must be used. The IPSec VPN connections on this security system always use the tunnel mode.

In transport mode, the original IP packet is not encapsulated in another packet. The original IP header is retained, and the rest of the packet is sent either in clear text (AH) or encrypted (ESP). Either the complete packet can be authenticated with AH, or the payload can be encrypted and authenticated using ESP. In both cases, the original header is sent over the WAN in clear text.

In tunnel mode, the complete packet—header and payload—is encapsulated in a new IP packet. An IP header is added to the IP packet, with the destination address set to the receiving tunnel endpoint. The IP addresses of the encapsulated packets remain unchanged. The original packet is then authenticated with AH or encrypted and authenticated using ESP.

IPSec Protocols

IPSec uses two protocols to communicate securely on the IP level.

- **Authentication Header (AH):** A protocol for the authentication of packet senders and for ensuring the integrity of packet data.
- **Encapsulating Security Payload (ESP):** A protocol for encrypting the entire packet and for the authentication of its contents.

The *Authentication Header* protocol (AH) checks the authenticity and integrity of packet data. In addition, it checks that the sender and receiver IP addresses have not been changed in transmission. Packets are authenticated using a checksum created using a *Hash-based Message Authentication Code* (HMAC) in connection with a key. One of the following hashing algorithms will be used:

- **Message Digest Version 5 (MD5):** This algorithm generates a 128-bit checksum from a message of any size. This checksum is like a fingerprint of the message, and will change if the message is altered. This hash value is sometimes also called a digital signature or a message digest.
- **The Secure Hash (SHA-1):** This algorithm generates a hash similar to that of MD5, though the SHA-1 hash is 160 bits long. SHA-1 is more secure than MD5, due to its longer key.

Compared to MD5, an SHA-1 hash is somewhat harder to compute, and requires more CPU time to generate. The computation speed depends, of course, on the processor speed and the number of IPSec VPN connections in use at the Astaro Security Gateway.

In addition to encryption, the *Encapsulated Security Payload* protocol (ESP) offers the ability to authenticate senders and verify packet contents. If ESP is used in tunnel mode, the complete IP packet (header and payload) is encrypted. New, unencrypted IP and ESP headers are added to the encapsulating packet: The new IP header contains the address of the receiving gateway and the address of the sending gateway. These IP addresses are those of the VPN tunnel.

For ESP with encryption normally the following algorithms are used:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Of these, AES offers the highest standard of security. The effective key lengths that can be used with AES are 128, 192 and 256 bits. Astaro Security Gateway supports a number of encryption algorithms. Either the MD5 or SHA-1 algorithms can be used for authentication.

NAT Traversal (NAT-T)

NAT traversal is a technology for establishing connections between hosts in TCP/IP networks which use NAT devices. This is achieved by using UDP encapsulation of the ESP packets to establish IPSec tunnels through NAT devices. UDP encapsulation is only used if NAT is detected between the IPSec peers; otherwise normal ESP packets will be used.

With NAT traversal you are able to place the firewall or a road warrior behind a NAT router and still establish an IPSec tunnel. Both IPSec peers must support NAT traversal if you want to use this feature, which is automatically negotiated. Make sure that the NAT device has IPSec-passthrough turned off, because this could impair the use of NAT traversal.

If road warriors want to use NAT traversal, their corresponding user object in WebAdmin must have a static remote access IP address (RAS address) set (see also *Use Static Remote Access IP* on the user definitions page in WebAdmin).

By default, a NAT traversal keep-alive signal is sent at intervals of 60 seconds to prevent an established tunnel from expiring when no data is transmitted. The keep-alive messages are sent to ensure that the NAT router keeps the state information associated with the session so that the tunnel stays open.

Connections

On the *Site-to-site VPN >> IPSec >> Connections* tab you can create and edit IPSec connections.

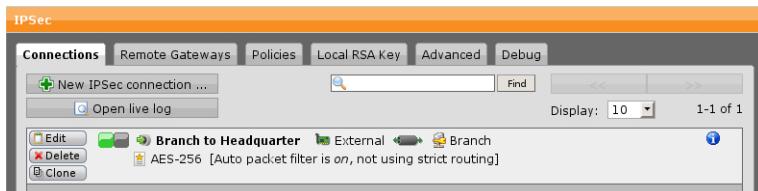


Figure 15.1 IPSec Connections List

To create an IPSec connection, proceed as follows:

1. On the **Connections** tab, click **New IPSec Connection**.

The Add IPSec Connection dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for this connection.

Remote Gateway: Select a remote gateway definition. Remote gateways are configured on the *Site-to-site VPN >> IPSec >> Remote Gateways* tab.

Local Interface: Select the name of the interface which is used as the local endpoint of the IPSec tunnel.

Policy: Select the IPSec policy for this IPSec connection. IPSec policies can be defined on the *Site-to-site VPN >> IPSec >> Policies* tab.

Local Networks: Select the local networks that should be reachable through the VPN tunnel.

Auto Packet Filter: By selecting this option you can automatically add packet filter rules that allow traffic for the VPN connection. The rules are added as soon as the VPN connection is successfully established, and they are removed when the VPN connection is disconnected. If you want to use a stricter IPSec connection, disable *Auto Packet Filter* and use IPSec objects in the packet filter ruleset instead.

Strict Routing: If strict routing is enabled, VPN routing is done according to source and destination IP address (instead of only destination IP address). In this case, only those packets exactly matching the VPN tunnel definition are routed into the VPN tunnel. As a consequence, you cannot use SNAT to add networks or hosts to the VPN tunnel, that are originally not part of the tunnel definition. On the other hand, without strict routing, you cannot have a mixed unencrypted/encrypted setup to the same network from different source addresses.

Comment (optional): Add a description or other information about the IPSec connection.

3. Click **Save**.

The new connection appears on the IPSec *Connections* list.

To either edit or delete a connection, click the corresponding buttons.

Open Live Log: The IPSec VPN live log displays monitoring information about established IPSec connection. Click the button to open it in a new window.

Remote Gateways

On the *Site-to-site VPN >> Remote Gateways* tab you can define the remote gateways for your site-to-site VPN tunnels. These remote network definitions

will become available when creating IPSec connections on the *IPSec >> Connections* tab.

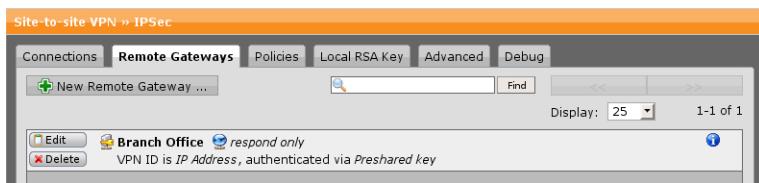


Figure 15.2 IPSec Remote Gateway List

To add a remote gateway, proceed as follows:

1. **On the *Remote Gateways* tab, click *New Remote Gateway*.**

The *Add Remote Gateway* dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for this remote gateway.

Gateway Type: Select the type of the gateway. The following types are available:

- **Initiate Connection:** Select if the remote endpoint has a static IP address so that a connection to the remote gateway can be initiated by the firewall. If selected, specify the remote gateway in the *Gateway* box. Note that you can also select this option if the remote gateway is resolved through DynDNS.
- **Respond Only:** Select if the IP address of the remote endpoint is unknown or cannot be resolved through DynDNS. The firewall is not able to initiate a connection to the remote gateway but waits for incoming connections to which it only needs to respond.

Authentication Type: Select the authentication type for this remote gateway definition. The following types are available:

- **Preshared key:** Authentication with *Preshared Keys* (PSK) uses secret passwords as keys. These passwords must be distributed to the endpoints before establishing the connection. When a new VPN tunnel is established, each side checks that the other knows the secret password. The security of PSKs depends on the quality of the passwords used: common words and phrases are subject to dictionary attacks. Permanent or long-term IPSec connections should use certificates or RSA keys instead.
- **RSA Key:** Authentication using RSA keys is much more sophisticated. In this scheme, each side of the connection generates a key pair consisting

of a public key and a private key. The private key is necessary for the encryption and authentication during the key exchange. Both endpoints of an IPSec VPN connection using this authentication method need their own key pair. Copy the public RSA key of the remote unit (*Site-to-site VPN >> IPSec >> Local RSA Key*) into the *Public Key* box of the local unit and vice versa. In addition, enter the VPN ID types and VPN identifiers that correspond to the respective RSA keys.

- **Local X.509 Certificate:** Similarly, the X.509 certificate authentication scheme uses public keys and private keys. An X.509 certificate contains the public key together with information identifying the owner of the key. Such certificates are signed and issued by a trusted *Certificate Authority* (CA). During the key exchange process, the certificates are exchanged and authenticated using a locally stored CA certificate. Select this authentication type if the X.509 certificate of the remote gateway is locally stored on the unit.
- **Remote X.509 Certificate:** Select this authentication type if the X.509 certificate of the remote gateway is not locally stored on the unit. You must then select the VPN ID type and VPN identifier of the certificate being used on the remote unit, that is, the certificate which is selected in the *Local X.509 Certificate* area of the *Site-to-site VPN >> IPSec >> Advanced* tab.

Enable XAUTH Client Mode: XAUTH is an extension of IPsec IKE to authenticate users via username and password at a VPN gateway. To use XAUTH for authentication with this remote gateway, select the option and provide username and password (twice) as required by the remote gateway.

VPN ID Type: Depending on the authentication type you must select a VPN ID type and VPN identifier. The VPN identifier entered here must match the values configured on the remote site. Suppose you are using two ASG appliances for establishing a site-to-site VPN tunnel. If you select *RSA Key* as authentication type on the local unit, the VPN ID type and the VPN identifier must match what is configured on the *Site-to-site VPN >> IPSec >> Local RSA Key* tab on the remote unit.

You can select among the following VPN ID types:

- IP address
- Hostname

- E-mail address
- Distinguished name (only available if authentication type is set to *Remote X.509 Certificate*)

Remote Networks: Select the remote networks that should be reachable via the remote gateway.

Comment (optional): Add a description or other information about the remote gateway.

3. Click Save.

The gateway definition appears on the *Remote Gateways* list.

To either edit or delete a remote gateway definition, click the corresponding buttons.

Policies

On the *IPSec >> Policies* tab you can customize parameters for IPSec connections and unite them into a policy. An IPSec policy defines IKE (Internet Key Exchange) and IPSec proposal parameters of an IPSec connection. Note that each IPSec connection needs an IPSec policy.

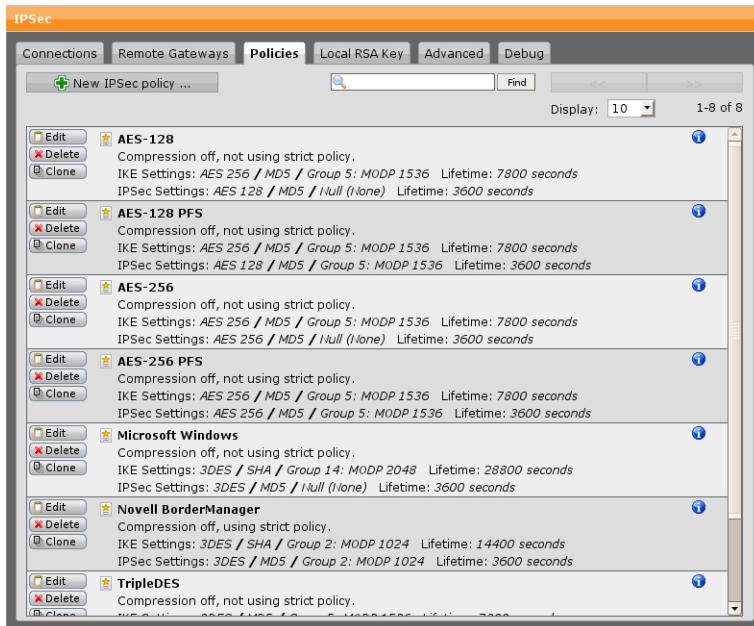


Figure 15.3 IPSec Policy List

To create a policy, proceed as follows:

1. **On the Policy tab, click New IPSec Policy.**

The Add IPSec Policy dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for this policy.

IKE Encryption Algorithm: The encryption algorithm specifies the algorithm used for encrypting the IKE messages. Supported algorithms are:

- *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 Authentication Algorithm: The authentication algorithm specifies the algorithm used for integrity checking of the IKE messages. Supported algorithms are:

- *MD5* (128 bit)
- *SHA* (160 bit)
- *SHA 256* (256 bit)
- *SHA 512* (512 bit)

IKE SA Lifetime: This value specifies the timeframe in seconds for which the IKE SA is valid and when the next rekeying should take place. Valid values are between 60 sec and 28800 sec (8 hrs). The default value is 7800 seconds.

IKE DH Group: When negotiating a connection, the communicating parties also settle the actual keys used to encrypt the data. In order to generate a session key, IKE uses the *Diffie-Hellman* (DH) algorithm, which utilizes random data. The random data generation is based on pool bits. The IKE

group basically tells the number of pool bits. The more pool bits, the larger the random numbers. The larger the numbers, the harder it is to crack the Diffie-Hellman algorithm. As a consequence, more pool bits mean more security but also the consumption of more CPU resources. Currently, the following Diffie-Hellman groups are supported:

- o Group 1: MODP 768
- o Group 2: MODP 1024
- o Group 5: MODP 1536
- o Group 14: MODP 2048
- o Group 15: MODP 3072
- o Group 16: MODP 4096

Note – Group 1 (MODP 768) is considered weak and only supported for interoperability reasons.

IPSec Encryption Algorithm: The same encryption algorithms as for IKE.

IPSec Authentication Algorithm: The same authentication algorithms as for IKE.

IPSec SA Lifetime: This value specifies the timeframe in seconds for which the IPSec SA is valid and when the next rekeying should take place. Valid values are between 60 sec and 86400 sec (1 day). The default value is 7800 seconds.

IPSec PFS Group: *Perfect Forward Secrecy* (PFS) refers to the notion that if a session key is compromised, it will permit access only to data of this specific session. In order for PFS to exist, the key used to protect the IPSec SA must not be derived from random keying material used to get the keys for the IKE SA. Therefore, PFS initiates a second Diffie-Hellman key exchange proposing the selected DH group for the IPSec connection to get a new randomly generated key. Supported Diffie-Hellman groups are the same as for IKE.

Enabling PFS is considered to be more secure, but it takes also more time for the exchange. It is not recommended to use PFS on slow hardware.

Note – PFS is not fully interoperable with all vendors. If you notice problems during the negotiation, you might consider disabling PFS.

Strict Policy: If an IPSec gateway makes a proposition with respect to an encryption algorithm and to the strength, it might happen that the gateway of the receiver accepts this proposition, even though the IPSec policy does not correspond to it. If you select this option and the remote endpoint does not agree on using exactly the parameters you specified, the IPSec connection will not be established. Suppose the IPSec policy of your security system requires AES-256 encryption, whereas, for example, a road warrior with SSH Sentinel wants to connect with AES-128; with the strict policy option enabled, the connection would be rejected.

Note – The compression setting will not be enforced via *Strict Policy*.

Compression: This option specifies whether IP packets should be compressed by means of the *IP Payload Compression Protocol* (IPComp) prior to encryption. IPComp reduces the size of IP packets by compressing them to increase the overall communication performance between a pair of communicating hosts or gateways. Compression is turned off by default.

Comment (optional): Add a description or other information about the policy.

3. Click **Save**.

The new IPSec policy appears on the IPSec *Policies* list.

To either edit or delete a policy, click the corresponding buttons.

Local RSA Key

With RSA authentication, RSA keys are used for authentication of the VPN endpoints. The public keys of the endpoints are exchanged manually before the connection is established. If you want to use this authentication type, you have to define a VPN identifier and create a local RSA key. The public RSA key of the firewall must be made available to remote IPSec devices that use IPSec RSA authentication with Astaro Security Gateway.

Current Local Public RSA Key: Displayed is the public portion of the currently installed local RSA key pair. Click into the box, then press CTRL-a and CTRL-c to copy it to the clipboard.

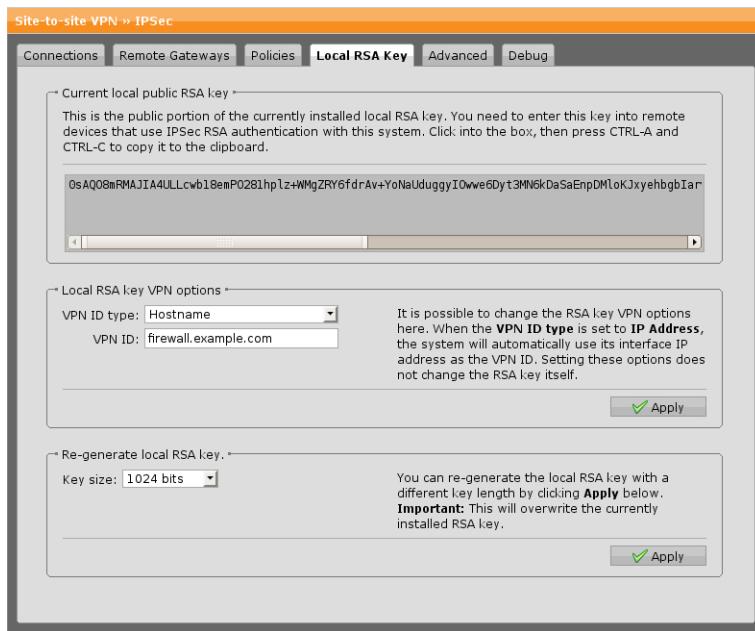


Figure 15.4 Configuring the Local RSA Key

Local RSA Key VPN Options: Select the VPN ID type which best suits your needs. By default, the hostname of the firewall is taken as the VPN identifier. If you have a static IP address as local VPN endpoint, select **IP Address**. Alternatively, use an e-mail address as VPN ID for mobile IPSec road warriors.

- **Hostname:** Default setting; the hostname of the firewall. However, you can enter a different hostname here.
- **E-mail Address:** By default, this is the e-mail address of the firewall's admin account. However, you can enter a different e-mail address here.
- **IP Address:** The IP address of the external interface of the firewall.

Click **Apply** to save your settings. Changing the settings does not modify the RSA key.

Re-generate Local RSA Key: To generate a new RSA key, select the desired key size and click **Apply**. This will start the key generation process, which can take from a few minutes up to two hours, according to your selected key length and used hardware. The key size (key length) is a measure of the number of

keys which are possible with a cipher. The length is usually specified in bits. The following key sizes are supported:

- 1024 bits
- 2048 bits
- 4096 bits

Once the RSA key has been generated, the appropriate public key will be displayed in the *Current Local Public RSA Key* box. Generating a new RSA key will overwrite the old one.

Advanced

On the *Site-to-site VPN >> IPSec >> Advanced* tab you can configure advanced options of IPSec VPN. Depending on your preferred authentication type, you can define the local certificate (for X.509 authentication) and the local RSA key (for RSA authentication), among other things. Note that this should only be done by experienced users.

Local X.509 Certificate

With X.509 authentication, certificates are used to verify the public keys of the VPN endpoints. If you want to use this authentication type, you have to select a local certificate from the drop-down list in the *Local X.509 Certificate* area. The selected key/certificate is then used to authenticate the firewall to remote peers if X.509 authentication is selected.

You can only select certificates where the appropriate private key is present, other certificates are not available in the drop-down list.

If there is no certificate available for selection, you have to add one in the *Certitificate Management* menu, either by creating a new one or by importing one using the upload function.

After selecting the certificate, enter the passphrase the private key was protected with. During the saving process, the passphrase is verified and an error message is displayed if it does not match the encrypted key.

Once an active key/certificate is selected, it is displayed in the *Local X.509 Certificate* area.

Dead Peer Detection (DPD)

Use Dead Peer Detection: The dead peer detection option is used for automatically terminating a connection if the remote VPN gateway or client is unreachable. For connections with static endpoints, the tunnel will be re-negotiated

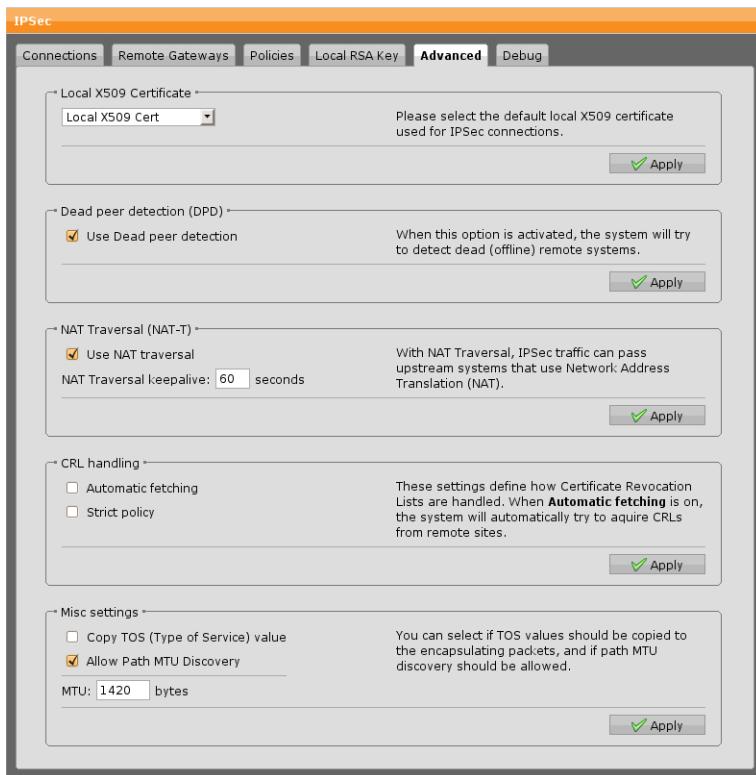


Figure 15.5 Configuring Advanced IPSec Site-to-site VPN Settings

automatically. Connections with dynamic endpoints require the remote side to re-negotiate the tunnel. Usually it is safe to always enable this option. The IPSec peers automatically determine whether the remote side supports dead peer detection or not, and will fall back to normal mode if necessary.

NAT Traversal (NAT-T)

Use NAT Traversal: Select to enable that IPSec traffic can pass upstream systems which use *Network Address Translation* (NAT). Additionally, you can define the keepalive interval for NAT traversal. Click *Apply* to save your settings.

CRL Handling

Automatic Fetching: There might be situations in which the provider of a certificate attempts to revoke the confirmation awarded with still valid certificates, for example if it has become known that the receiver of the certificate fraudulently obtained it by using wrong data (name, etc.) or because an attacker has got hold of the private key, which is part of the certified public key. For

this purpose, so-called *Certificate Revocation Lists* or CRLs are used. They normally contain the serial numbers of those certificates of a certifying instance, that have been held invalid and that are still valid according to their respective periods of validity.

After the expiration of these periods the certificate will no longer be valid and must therefore not be maintained in the block list. The *Automatic CRL Fetching* function automatically requests the CRL through the URL defined in the partner certificate via HTTP, Anonymous FTP or LDAP version 3. On request, the CRL can be downloaded, saved and updated, once the validity period has expired. If you use this feature, make sure that you set the packet filter rules accordingly, so that the CRL distribution server can be accessed.

Strict Policy: If this option is enabled, any partner certificate without a corresponding CRL will be rejected.

Misc Settings

Copy TOS Flag: Type of Service bits (TOS bits) are several four-bit flags in the IP header. These bits are referred to as *Type of Service* bits because they allow the transferring application to tell the network which type of service quality is necessary. The following service types are available:

- Minimize delay (binary number: 1000)
- Maximize throughput (binary number: 0100)
- Maximize reliability (binary number: 0010)
- Minimize monetary cost (binary number: 0001)
- Normal service (binary number: 0000)

Enabling this option will copy the content of the *Type of Service* field into the encrypted data packet, so that the IPSec data traffic can be routed according to its priority.

Allow Path MTU Discovery: It is usually preferable that IP data packets be of the largest size that does not require fragmentation anywhere along the path from the source to the destination. This size of the data packet is referred to as the *Path Maximum Transmission Unit* (PMTU). If any of the data packets are too large to be forwarded without fragmentation by some router along the path, that router will discard them and return *ICMP Destination Unreachable* messages with a code meaning "fragmentation needed and DF set". Upon receipt of such a message, the source host reduces its assumed PMTU for the path.

MTU: In this field you can specify the *Maximum Transmission Unit* (MTU) of the IPSec interface; the default MTU is 1420 byte.

Debug

On the *IPSec >> Debug* tab you can configure basic IKE debug options. Select the checkboxes for which types of IKE messages you want to create debug output. The following flags can be logged:

- **Control:** Displays control messages of IKE state
- **Emitting:** Displays content of outgoing IKE messages
- **Parsing:** Displays content of incoming IKE messages
- **Raw:** Displays messages as raw bytes
- **Crypt:** Shows encryption and decryption operations

SSL

Site-to-site VPN tunnels can be established via an SSL connection. SSL VPN connections have distinct roles attached. The tunnel endpoints act as either client or server. The client always initiates the connection, the server responds to client requests. Keep in mind that this contrasts IPSec where both endpoints normally can initiate a connection.

Note – If you run into problems in establishing a connection, check whether SSL scanning is activated with the HTTP proxy operating in transparent mode. If so, make sure that the target host of the VPN connection has been added to the *Transparent Mode SkipList* under *Web Security >> HTTP/S >> Advanced*.

Connections

To create an SSL VPN site-to-site tunnel, it is crucial to create the server configuration first. The configuration of the client has always to be the second step.

To create the server configuration, proceed as follows:

1. On the **Connections** tab, click **New SSL Connection**.

The Add SSL Connection dialog box opens.

2. Make the following settings:

Connection Type: Select *Server* from the drop-down list.

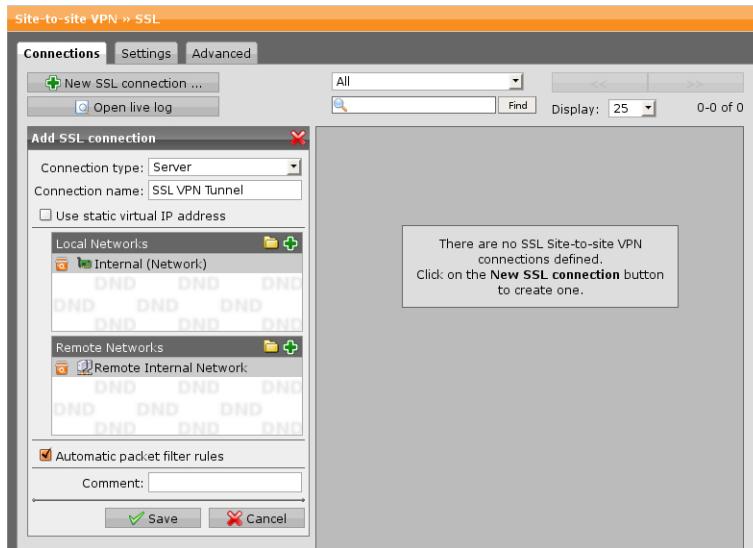


Figure 15.6 SSL VPN Connection Server Configuration

Connection Name: Enter a descriptive name for the connection.

Use Static Virtual IP Address (optional): Only select this option if the IP address pool is not compatible with the client's network environment: By default clients are assigned an IP address from the *Virtual IP Pool* (configurable on *Settings* tab). Rarely, it may happen that such an IP address is already in use on the client's host. In that case enter a suitable IP address in the *Static Peer IP* field which will then be assigned to the client during tunnel setup.

Local Networks: Add one or more local networks that are allowed to be accessed remotely.

Remote Networks: Add one or more remote networks that are allowed to connect to the local network(s).

Note – You can change the *Local Networks* and *Remote Networks* settings later without having to reconfigure the client.

Automatic Packet Filter Rules (optional): When enabled, the security system will automatically allow access to the selected local networks for all accessing SSL VPN clients.

Comment (optional): Add a description or other information about the SSL connection.

3. Click Save.

The new SSL server connection appears on the *Connections* list.

4. Download the configuration file.

Use the *Download* button, which is located in the newly created SSL server connection row, to download the client configuration file for this connection.

Encrypt Configuration File: It is advisable to encrypt the configuration file for security reasons. Enter a password twice.

Click *Download Peer Config* to save the file.

This file is needed by the client-side administrator in order to be able to set up the client endpoint of the tunnel.

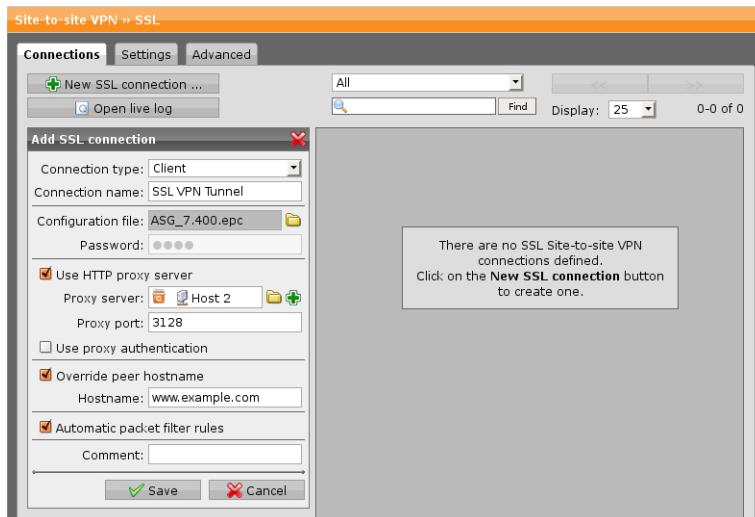


Figure 15.7 SSL VPN Connection Client Configuration

The next step is the client configuration which has to take place on client side and *not* on server side. Ensure that the downloaded client configuration file is at hand.

To create the client configuration, proceed as follows:

1. On the *Connections* tab, click *New SSL Connection*.

The *Add SSL Connection* dialog box opens.

2. Make the following settings:

Connection Type: Select *Client* from the drop-down list.

Connection Name: Enter a descriptive name for the connection.

Configuration File: Click the folder icon, browse for the client configuration file and click *Save*.

Password (optional): If the file has been encrypted, enter the password.

Use HTTP Proxy Server (optional): Select the checkbox if the client is located behind a proxy and enter the settings for the proxy.

Use Proxy Authentication (optional): Select the checkbox if the client needs to authenticate against the proxy and enter username and password.

Override Peer Hostname: Select the checkbox and enter a hostname here if the server system's regular hostname (or DynDNS hostname) cannot be resolved from the client host.

Automatic Packet Filter Rules (optional): When enabled, the security system will automatically allow traffic between hosts on the tunneled local and remote networks.

Comment (optional): Add a description or other information about the SSL connection.

3. Click **Save**.

The new SSL VPN client connection appears on the *Connections* list.

To either edit or delete , click the corresponding buttons.

Click on the *Site-to-site VPN* menu to see the status of the SSL VPN connection on the overview page. The status icon there turns green when the connection is established. Then information about the interconnected subnets on both sides of the tunnel becomes available, too.

Settings

On the *SSL >> Settings* tab you can configure the basic settings for SSL VPN server connections.

Note – This tab is identical for *Site-to-site VPN >> SSL* and *Remote Access >> SSL*. Changes applied here always affect both SSL configurations.

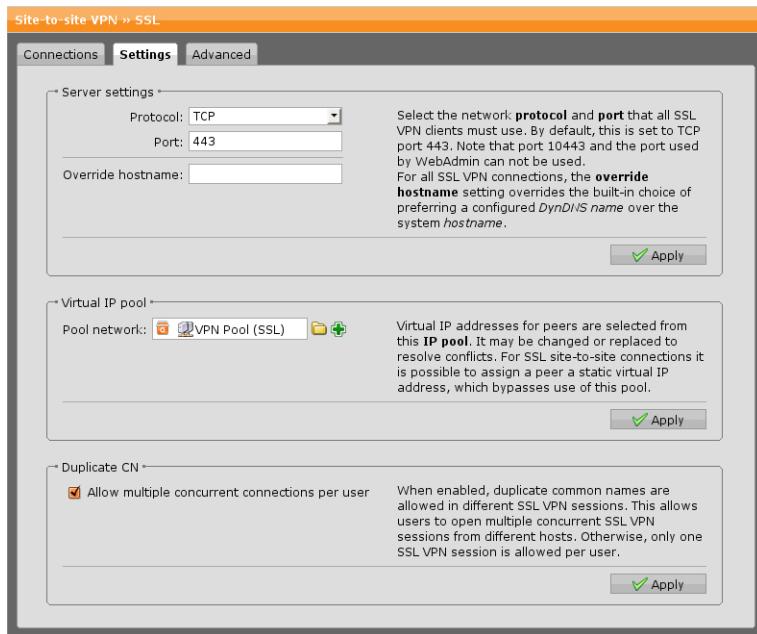


Figure 15.8 Configuring SSL Site-to-site VPN Settings

Server Settings

You can make the following settings for the SSL VPN connection:

- **Protocol:** Select the protocol to use. You can choose either *TCP* or *UDP*.
- **Port:** You can change the port. The default port is 443. You cannot use port 10443, the ACC Gateway Manager port 4422, or the port used by the WebAdmin interface.
- **Override Hostname:** The value in the *Override Hostname* box is used as the target hostname for client VPN connections and is by default the hostname of the firewall. Only change the default if the system's regular hostname (or DynDNS hostname) cannot be reached under this name from the Internet.

Virtual IP Pool

Pool Network: This is the virtual IP address pool which is used to distribute IP addresses from a certain IP range to the SSL clients. By default, the *VPN Pool (SSL)* is selected. In case you select a different address pool, the netmask must not be greater than 29 bits, for OpenVPN cannot handle address pools whose netmask is /30, /31, or /32.

Duplicate CN

Select *Allow Multiple Concurrent Connections Per User* if you want to allow your users to connect from different IP addresses at the same time. When disabled, only one concurrent SSL VPN connection is allowed per user.

Advanced

On the *SSL >> Advanced* tab you can configure various advanced server options ranging from the cryptographic settings, through compression settings, to debug settings.

Note – This tab is identical for *Site-to-site VPN >> SSL* and *Remote Access >> SSL*. Changes applied here always affect both SSL configurations.

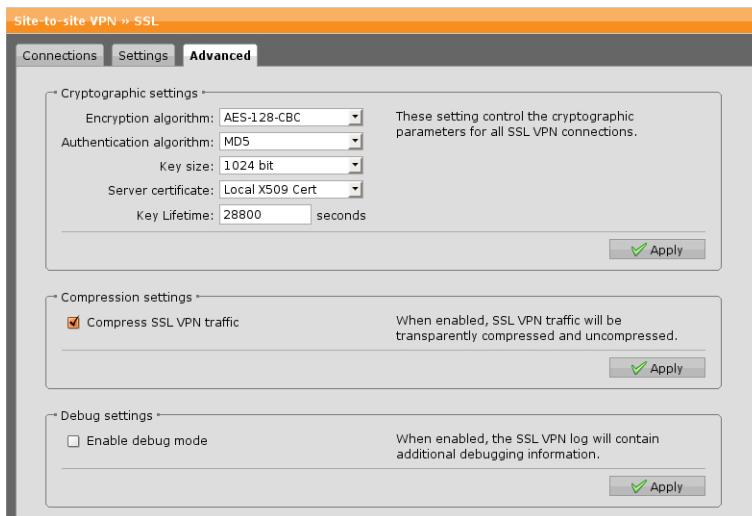


Figure 15.9 Configuring Advanced SSL Site-to-site VPN Settings

Cryptographic Settings

These settings control the encryption parameters for all SSL VPN remote access clients:

- Encryption Algorithm:** The encryption algorithm specifies the algorithm used for encrypting the data sent through the VPN tunnel. The following algorithms are supported, which are all in *Cipher Block Chaining* (CBC) mode:

- *DES-EDE3-CBC*
 - *AES-128-CBC* (128 bit)
 - *AES-192-CBC* (192 bit)
 - *AES-256-CBC* (256 bit)
 - *BF-CBC* (Blowfish (128 bit))
- **Authentication Algorithm:** The authentication algorithm specifies the algorithm used for checking the integrity of the data sent through the VPN tunnel. Supported algorithms are:
 - *MD5* (128 bit)
 - *SHA-1* (160 bit)
 - **Key Size:** The key size (key length) is the length of the Diffie-Hellman key exchange. The longer this key is, the more secure the symmetric keys are. The length is specified in bits. You can choose between a key size of 1024 or 2048 bits.
 - **Server Certificate:** Select a local SSL certificate to be used by the SSL VPN server to identify itself against the clients.
 - **Key Lifetime:** Enter a time period after which the key will expire. The default is 28,800 seconds.

Compression Settings

Compress SSL VPN Traffic: When enabled, all data sent through SSL VPN tunnels will be compressed prior to encryption.

Debug Settings

Enable Debug Mode: When enabling debug mode, the SSL VPN log file will contain extended information useful for debugging purposes.

Certificate Management

The *Site-to-site VPN >> Certificate Management* menu is the central place to manage all certificate-related operations of Astaro Security Gateway. This includes creating or importing X.509 certificates as well as uploading so-called *Certificate Revocation Lists* (CRLs), among other things.

Certificates

On the *Site-to-site VPN >> Certificate Management >> Certificates* tab you can create or import public key certificates in the X.509 standard format. Such certificates are digitally signed statements usually issued by a *Certificate Authority* (CA) binding together a public key with a particular *distinguished name* (DN) in X.500 notation.

All certificates you create on this tab are self-signed by the *Certificate Authority* (CA) that was created automatically using the information you provided during the initial login to the WebAdmin interface.

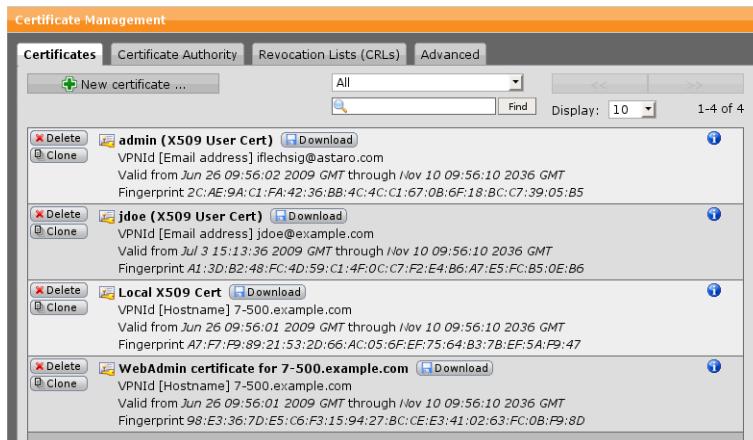


Figure 15.10 Site-to-site VPN Certificates List

To generate a certificate, proceed as follows:

1. **On the Certificates tab, click New Certificate.**

The Add Certificate dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for this certificate.

Method: To create a certificate, select Generate (for more information on

uploading certificates, see below).

Provide the following information:

- **VPN ID Type:** You have to define a unique identifier for the certificate. The following types of identifiers are available:

- Email Address
- Hostname
- IP Address
- Distinguished Name

- **VPN ID:** Depending on the selected VPN ID type, enter the appropriate value into this text box. For example, if you selected *IP Address* from the *VPN ID Type* list, enter an IP address into this text box. Note that this text box will be hidden when you select *Distinguished Name* from the *VPN ID Type* list.

Use the drop-down lists and text boxes from *Country* to *Email* to enter identifying information about the certificate holder. This information is used to build the *Distinguished Name*, that is, the name of the entity whose public key the certificate identifies. This name contains a lot of personal information in the X.500 standard and is supposed to be unique across the Internet. If the certificate is for a road warrior connection, enter the name of the user in the *Common Name* box. If the certificate is for a host, enter a hostname.

Comment (optional): Add a description or other information about the certificate.

3. Click Save.

The certificate appears on the *Certificates* list.

To delete a certificate click the button *Delete* of the respective certificate.

Alternatively, to upload a certificate, proceed as follows:

1. On the *Certificates* tab, click *New Certificate*.

The *Add Certificate* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for this certificate.

Method: Select *Upload*.

File Type: Select the file type of the certificate. You can upload certificates being one of the following types:

- **PKCS#12 Container:** PKCS refers to a group of *Public Key Cryptography Standards* (PKCS) devised and published by RSA laboratories. The PKCS#12 file format is commonly used to store private keys with accompanying public key certificates protected with a container passphrase. You must know this container passphrase to upload files in this format (enter the passphrase twice for verification).
- **PEM encoded:** A Base64 encoded *Privacy Enhanced Mail* (PEM) file format with no password required.

File: Click the folder icon next to the *File* box and select the certificate you want to upload.

Comment (optional): Add a description or other information about the certificate.

3. Click **Save**.

The certificate appears on the *Certificates* list.

To delete a certificate click the button *Delete* of the respective certificate.

You can download the certificate either in PKCS#12 or as PEM format. The PEM file only contains the certificate itself, while the PKCS#12 file also contains the private key as well as the CA certificate with which it was signed.

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

Certificate Authority

On the *Site-to-site VPN >> Certificate Management >> Certificate Authority* tab you can add new *Certificate Authorities* to the unit. Generally speaking, a certificate authority or *Certification Authority* (CA) is an entity which issues digital certificates for use by other parties. A CA attests that the public key contained in the certificate belongs to the person, organization, host, or other entity noted in the certificate by signing the certificate signing request with the

private key of the CA's own certificate. Such a CA is therefore called a signing CA.

On this security system, the signing CA was created automatically using the information you provided during the initial login to the security system. Thus, all certificates you create on the *Certificates* tab are self-signed certificates, meaning that the issuer and the subject are identical. However, you can alternatively import a signing CA by third-party vendors. In addition, to verify the authenticity of a host or user requesting an IPSec connection, you can also use alternative CA certificates whose private keys are unknown. Those CA certificates are called verification CAs and can be added on this tab as well.

Important – You can have multiple verification CAs on your system, but only one signing CA. So if you upload a new signing CA, the previously installed signing CA automatically becomes a verification CA.

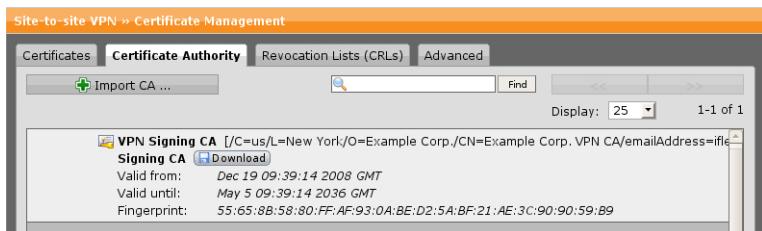


Figure 15.11 Certificate Authority List

To import a CA, proceed as follows:

1. On the **Certificate Authority** tab, click **Import CA**.

The *Import CA* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for this CA.

Type: Select the type of CA you are going to import. You can choose between verification CAs or signing CAs. A verification CA must be available in the PEM format, while a signing CA must be available in the PKCS#12 format.

CA Certificate: Click the folder icon next to the *CA Certificate* box and select the certificate you want to import. Note that if you are to upload a new signing CA, you must enter the password with which the PKCS#12 container was secured.

Comment (optional): Add a description or other information about the CA.

3. Click Save.

The new CA certificate appears on the *Certificate Authority* list.

To delete a CA click the button *Delete* of the respective CA.

The signing CA can be downloaded in PKCS#12 format. You will then be prompted to enter a password, which will be used to secure the PKCS#12 container. In addition, verification CAs can be downloaded in PEM format.

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

Revocation Lists

A Certificate Revocation List (CRL) is a list of certificates (more precisely, their serial numbers) which have been revoked, that is, are no longer valid, and should therefore not be relied upon. On the *Site-to-site VPN >> Certificate Management >> Revocation Lists (CRLs)* tab you can upload the CRL that is deployed within your public key infrastructure (PKI).

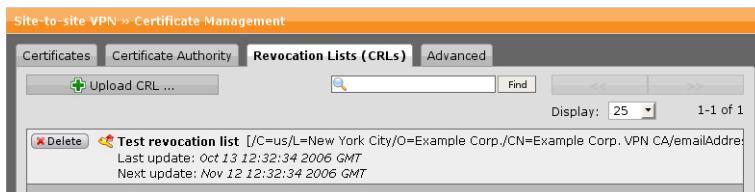


Figure 15.12 List of Revocation Lists (CRLs)

To upload a CRL, proceed as follows:

1. **On the Revocation Lists (CRLs) tab, click *Upload CRL*.**
The *Upload CRL* dialog box opens.
2. **Make the following settings:**
Name: Enter a descriptive name for this CRL.

CRL File: Click the folder icon next to the *CRL File* box and select the CRL you want to upload.

Comment (optional): Add a description or other information about the CRL.

3. Click Save.

The new CRL appears on the list of revocation lists.

To delete a CRL click the button *Delete* of the respective CRL.

Advanced

On the *Site-to-site VPN >> Certificate Management >> Advanced* tab you can regenerate the VPN Signing CA that was created during the initial setup of the unit. The VPN Signing CA is the certificate authority with which digital certificates are signed that are used for remote access and site-to-site VPN connections.

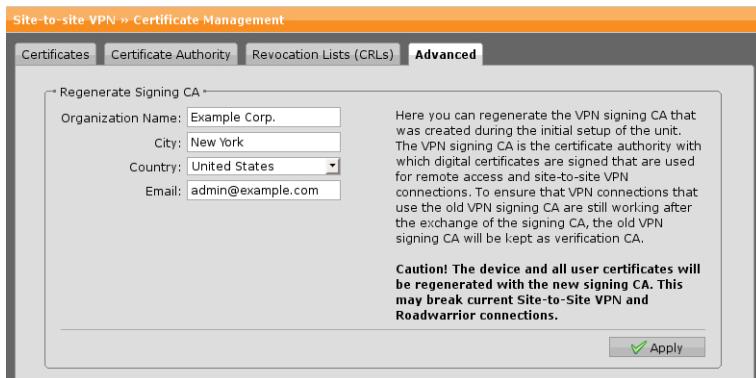


Figure 15.13 Advanced Settings

Regenerate Signing CA

You can renew all user certificates using the current signing CA. This becomes relevant once you have installed an alternative VPN Signing CA on the *Certificate Authority* tab.

Chapter 16

Remote Access

This chapter describes how to configure remote access settings of Astaro Security Gateway. Remote access using Astaro Security Gateway is realized by means of *Virtual Private Networks* (VPNs), which are a cost effective and secure way to provide remote users such as telecommuting employees access to the corporate network. VPNs use cryptographic tunneling protocols such as IPSec and PPTP to provide confidentiality and privacy of the data transmitted over them.

Cross Reference – More information on how to configure remote access VPN connections can be found in the Astaro knowledgebase³⁶ (navigate to *ASG Version 7 >> Astaro Manuals and Guides*).

The ASG automatically generates necessary installation and configuration files for the respective remote access connection type. Those files can be downloaded directly from the User Portal. However, only those files are available to a user that correspond to the connection types enabled for them, e.g., a user who has been enabled to use SSL remote access will find an SSL installation file only.

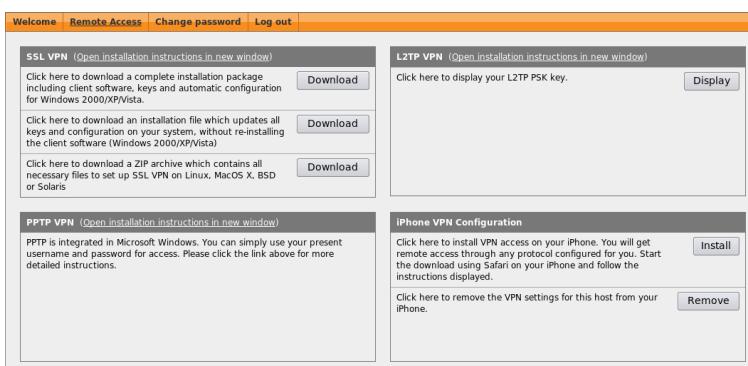


Figure 16.1 Remote Access Installation Files in User Portal

³⁶ <http://www.astaro.com/kb/>

The page *Remote Access Status* contains an overview of all online users.

The following topics are included in this chapter:

- SSL
- PPTP
- L2TP over IPSec
- IPSec
- Cisco VPN Client
- Advanced
- Certificate Management

SSL

The remote access SSL feature of Astaro Security Gateway is realized by OpenVPN, a full-featured SSL VPN solution. It provides the ability to create point-to-point encrypted tunnels between remote employees and your company, requiring both SSL certificates and a username/password combination for authentication to enable access to internal resources. In addition, it offers a secure User Portal, which can be accessed by each authorized user to download a customized SSL VPN client software bundle. This bundle includes a free SSL VPN client, SSL certificates and a configuration that can be handled by a simple one-click installation procedure. This SSL VPN client supports most business applications such as native Outlook, native Windows file sharing, and many more.

Cross Reference – More information on how to use the SSL VPN client can be found in the Astaro knowledgebase³⁷ (navigate to *ASG Version 7 >> Astaro Manuals and Guides*).

Global

On the *Remote Access >> SSL >> Global* tab you can configure the basic settings for the VPN access. By default, the SSL VPN solution of Astaro Security

³⁷ <http://astaro.com/kb>

Gateway employs so-called split tunneling, that is, the process of allowing a remote VPN user to access a public network, for example, the Internet, at the same time that the user is allowed to access resources on the VPN. However, split tunneling can be bypassed if you select *Any* in the Local Networks field below. Thus, all traffic will be routed through the VPN SSL tunnel. Whether users are allowed to access a public network then depends on your packet filter configuration.

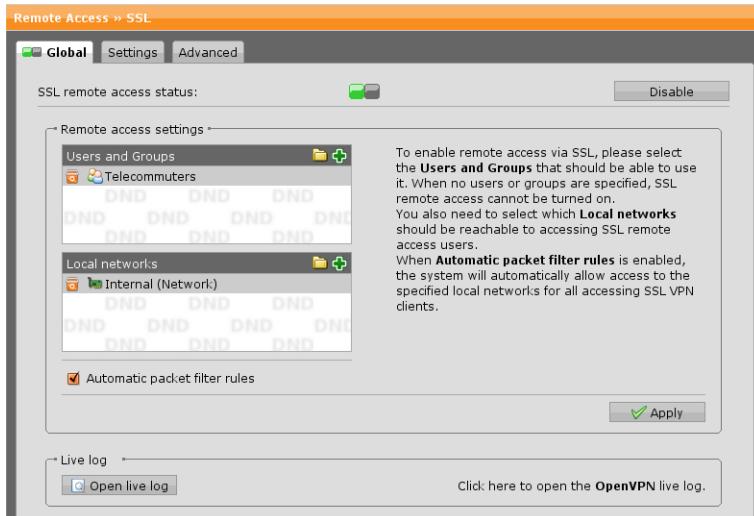


Figure 16.2 Configuring SSL Remote Access

To configure global SSL VPN options, proceed as follows:

1. On the *Global* tab, enable SSL remote access.

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *Remote Access Settings* area becomes editable.

2. Make the following settings:

Users and Groups: Select the users and user groups that should be able to use SSL VPN remote access. When no users or user groups are specified, SSL remote access cannot be enabled.

Note – The SSL VPN client software bundle in the User Portal is only available to users who are selected in the *Users and Groups* box and for whom a user definition does exist on the security system (tab *Users*). To users for

whom *only* a user definition is existent, no SSL VPN client software bundle is available. Nonetheless, they have access to the User Portal. The User Portal will show a note saying "Unfortunately this remote access method is not configured for you" on the *Remote Access >> SSL VPN* tab.

Local Networks: Select the local network(s) that should be reachable to SSL clients.

Automatic Packetfilter Rules: Select this option to have the necessary packetfilter rules automatically created.

3. Click **Apply**.

Your settings will be saved.

Open Live Log

The *OpenVPN Live Log* logs remote access activities. Click the button to open the live log in a new window.

Settings

On the *SSL >> Settings* tab you can configure the basic settings for SSL VPN server connections.

Note – This tab is identical for *Site-to-site VPN >> SSL* and *Remote Access >> SSL*. Changes applied here always affect both SSL configurations.

Server Settings

You can make the following settings for the SSL VPN connection:

- **Protocol:** Select the protocol to use. You can choose either *TCP* or *UDP*.
- **Port:** You can change the port. The default port is 443. You cannot use port 10443, the ACC Gateway Manager port 4422, or the port used by the WebAdmin interface.
- **Override Hostname:** The value in the *Override Hostname* box is used as the target hostname for client VPN connections and is by default the hostname of the firewall. Only change the default if the system's regular hostname (or DynDNS hostname) cannot be reached under this name from the Internet.

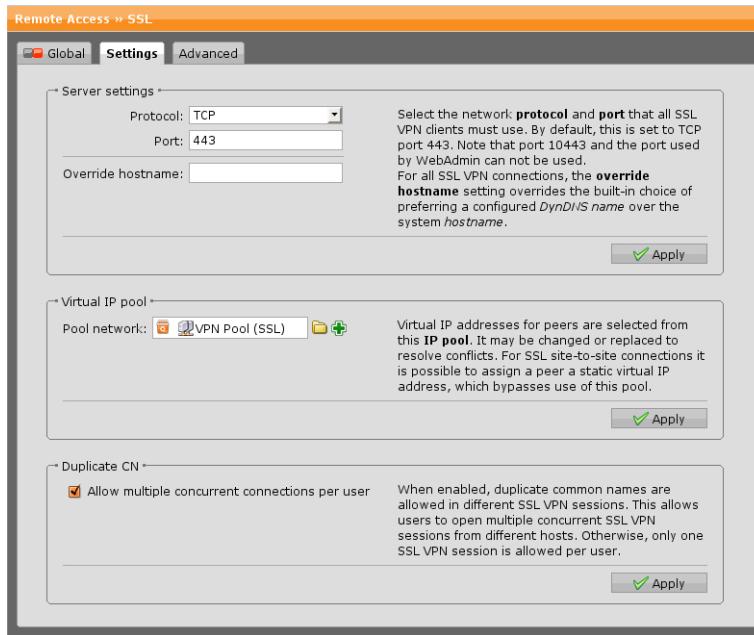


Figure 16.3 Configuring SSL Remote Access Settings

Virtual IP Pool

Pool Network: This is the virtual IP address pool which is used to distribute IP addresses from a certain IP range to the SSL clients. By default, the *VPN Pool (SSL)* is selected. In case you select a different address pool, the netmask must not be greater than 29 bits, for OpenVPN cannot handle address pools whose netmask is /30, /31, or /32.

Duplicate CN

Select *Allow Multiple Concurrent Connections Per User* if you want to allow your users to connect from different IP addresses at the same time. When disabled, only one concurrent SSL VPN connection is allowed per user.

Advanced

On the *SSL >> Advanced* tab you can configure various advanced server options ranging from the cryptographic settings, through compression settings, to debug settings.

Note – This tab is identical for *Site-to-site VPN >> SSL* and *Remote Access >> SSL*. Changes applied here always affect both SSL configurations.

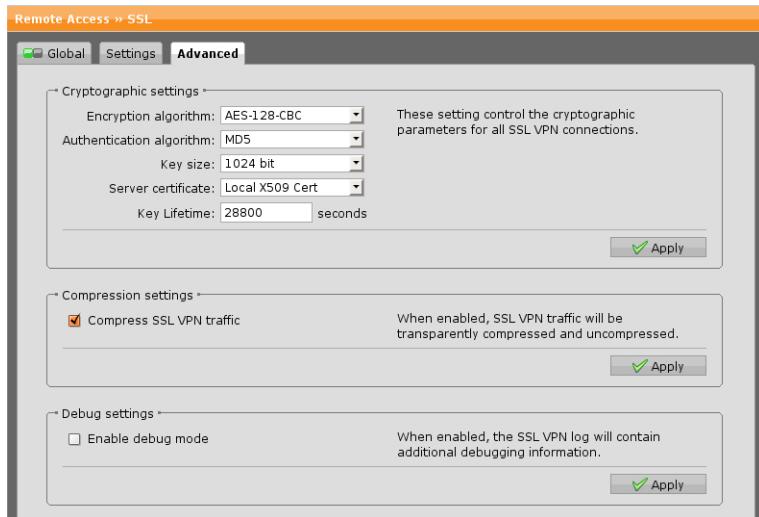


Figure 16.4 Configuring Advanced SSL Remote Access Settings

Cryptographic Settings

These settings control the encryption parameters for all SSL VPN remote access clients:

- **Encryption Algorithm:** The encryption algorithm specifies the algorithm used for encrypting the data sent through the VPN tunnel. The following algorithms are supported, which are all in *Cipher Block Chaining* (CBC) mode:
 - DES-EDE3-CBC
 - AES-128-CBC (128 bit)
 - AES-192-CBC (192 bit)
 - AES-256-CBC (256 bit)
 - BF-CBC (Blowfish (128 bit))
- **Authentication Algorithm:** The authentication algorithm specifies the algorithm used for checking the integrity of the data sent through the VPN tunnel. Supported algorithms are:

- MD5 (128 bit)
- SHA-1 (160 bit)
- **Key Size:** The key size (key length) is the length of the Diffie-Hellman key exchange. The longer this key is, the more secure the symmetric keys are. The length is specified in bits. You can choose between a key size of 1024 or 2048 bits.
- **Server Certificate:** Select a local SSL certificate to be used by the SSL VPN server to identify itself against the clients.
- **Key Lifetime:** Enter a time period after which the key will expire. The default is 28,800 seconds.

Compression Settings

Compress SSL VPN Traffic: When enabled, all data sent through SSL VPN tunnels will be compressed prior to encryption.

Debug Settings

Enable Debug Mode: When enabling debug mode, the SSL VPN log file will contain extended information useful for debugging purposes.

PPTP

Point-to-Point Tunneling Protocol (PPTP) allows single Internet-based hosts to access internal network services through an encrypted tunnel. PPTP is easy to configure and requires no special client software on Microsoft Windows systems.

PPTP is included with versions of Microsoft Windows starting with Windows 95. In order to use PPTP with Astaro Security Gateway, the client computer must support the MSCHAPv2 authentication protocol. Windows 95 and 98 users must apply an update to their systems in order to support this protocol.

Global

To configure global PPTP options, proceed as follows:

1. **On the *Global* tab, enable PPTP remote access.**

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *Main Settings* area becomes editable.

2. **Make the following settings:**

Authentication via: Select the authentication mechanism. PPTP remote access only supports local and RADIUS authentication.

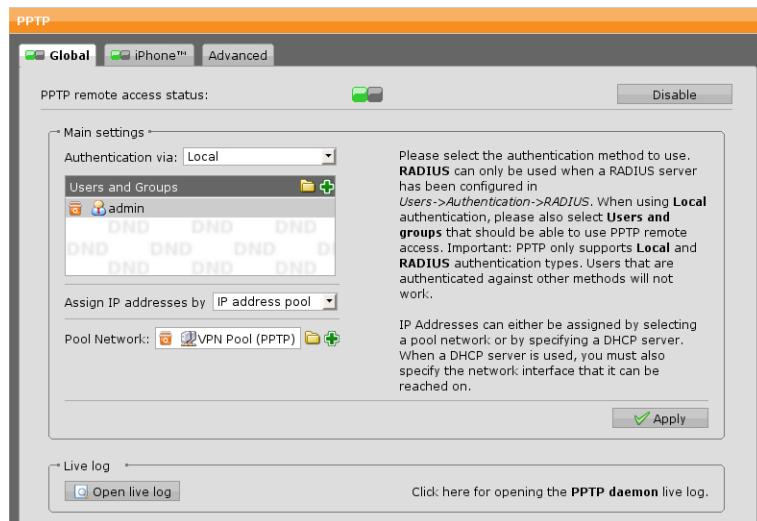


Figure 16.5 Configuring PPTP Remote Access

- **Local:** If you select *Local*, specify the users and user groups who should be able to use PPTP remote access. It is not possible to drag backend user groups into the field. Until a user account has been specified, PPTP remote access cannot be activated.

Note – Similar to SSL VPN the *Remote Access* menu of the User Portal can only be accessed by users who are selected in the *Users and Groups* box and for whom a user definition does exist on the security system. Otherwise the User Portal will display the note "Unfortunately this remote access method is not configured for you" on the *Remote Access >> PPTP VPN* tab. Authorized users who have successfully logged in to the User Portal will find a link to installation instructions, which are available at the Astaro knowledgebase³⁸ (navigate to *ASG Version 7 >> Remote Access >> PPTP*).

- **RADIUS:** *RADIUS* can only be selected if a RADIUS server has been previously configured. With this authentication method users will be authenticated against an external RADIUS server that can be configured on the *Users >> Authentication >> Servers* tab. The *Users and Groups*

³⁸ <http://www.astaro.com/kb>

dialog box will be grayed out. However, its settings can still be changed, which has no effect. The RADIUS server must support MSCHAPv2 challenge-response authentication. The server can pass back parameters such as the client's IP address and DNS/WINS server addresses. The PPTP module sends the following string as NAS-ID to the RADIUS server: pptp. Note that when RADIUS authentication is selected, local users cannot be authenticated with PPTP anymore. Note further that clients must support MSCHAPv2 authentication as well.

Assign IP addresses by: When enabling PPTP you can either assign IP addresses from a predefined IP address pool or distribute them automatically by means of a DHCP server. Thus, the following options can be selected:

- **IP Address Pool:** Select this option if you want to assign IP addresses from a certain IP range to the clients gaining remote access through PPTP. By default, addresses from the private IP space 10.242.1.0/24 are assigned. This network definition is called the *VPN Pool (PPTP)* and can be used in all network-specific configuration options. If you want to use a different network, simply change the definition of the *VPN Pool (PPTP)* on the *Definitions >> Networks* page. Alternatively, you can create another IP address pool by clicking the plus icon next to the *Pool Network* text box.
- **DHCP Server:** If you select this option, enter the following DHCP settings:
 - **DHCP Server:** The IP address of the DHCP server. Note that the local DHCP server is not supported. The DHCP server to be specified here must be running on a physically different system.
 - **on Interface:** The local interface through which the DHCP server is connected. Note that the DHCP server does not have to be directly connected to the interface — it can also be accessed through a router.

3. Click **Apply**.

Your settings will be saved.

Live Log

The *PPTP Daemon Live Log* logs all PPTP remote access activities. Click the button to open the live log in a new window.

iPhone

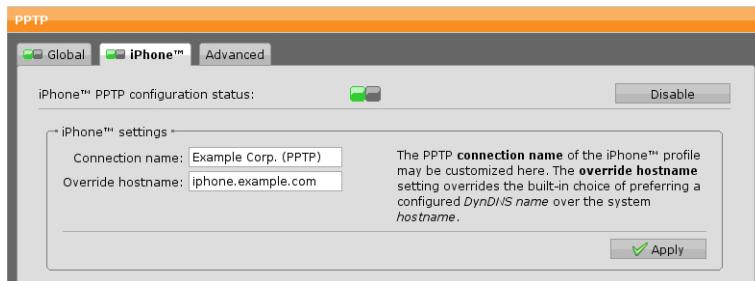


Figure 16.6 Configuring iPhone Remote Access Via PPTP

You can enable that iPhone users are offered automatic PPTP configuration in the User Portal.

However, only users that have been added to the *Users and Groups* box on the *Global* tab will find configuration files on their User Portal site. The iPhone status is enabled by default.

Connection Name: Enter a descriptive name for the PPTP connection so that iPhone users may identify the connection they are going to establish. The default name is your company name followed by the protocol PPTP.

Note – Connection Name must be unique among all iPhone connection settings (PPTP, L2TP over IPSec, Cisco VPN Client).

Override Hostname: In case the system hostname cannot be publicly resolved by the client, you can enter a server hostname here that overrides the internal preference of the *DynDNS Hostname* before the *System DNS Hostname*.

To disable automatic iPhone configuration, click the status icon or *Disable* in the header of the tab.

The status icon turns red.

Advanced

On the *Remote Access >> PPTP >> Advanced* tab you can configure the encryption strength and the amount of debug output with regard to PPTP remote access. Note that advanced PPTP options can only be configured if PPTP remote access status is enabled on the *Global* tab.

Encryption Strength

You can choose between strong (128-bit) and weak (40-bit) tunnel encryption

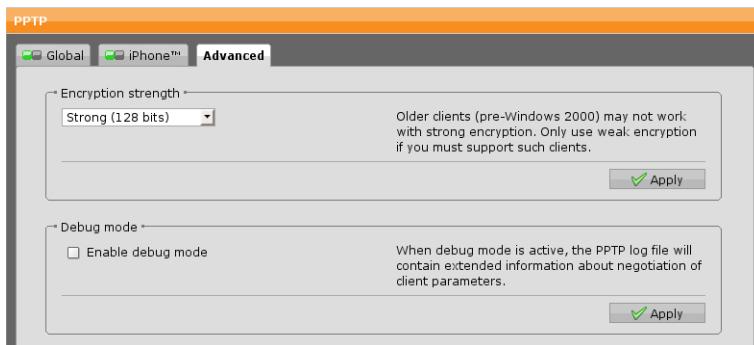


Figure 16.7 Configuring Advanced PPTP Remote Access Settings

(MPPE). Do not use weak encryption unless you have endpoints that do not support 128-bit encryption.

Debug Mode

Enable Debug Mode: This option controls how much debug output is generated in the PPTP log. Select this option if you encounter connection problems and need detailed information about the negotiation of client parameters, for example.

L2TP over IPSec

L2TP, short for *Layer Two (2) Tunneling Protocol*, is a data link layer (layer 2 of the OSI model) protocol for tunneling network traffic between two peers over an existing network (usually the Internet), better known as *Virtual Private Networks* (VPNs). Because of the lack of confidentiality inherent in the L2TP protocol, it is often combined with IPSec, which provides confidentiality, authentication, and integrity. The combination of these two protocols is also known as L2TP over IPSec. L2TP over IPSec allows you, while providing the same functions as PPTP, to give individual hosts access to your network through an encrypted IPSec tunnel.

Global

On the *L2TP over IPSec >> Global* tab you can configure basic options for setting up remote access via L2TP over IPSec.

To use L2TP over IPSec, proceed as follows:

1. **On the *Global* tab enable L2TP over IPSec.**

You can either click the status icon or the *Enable* button.

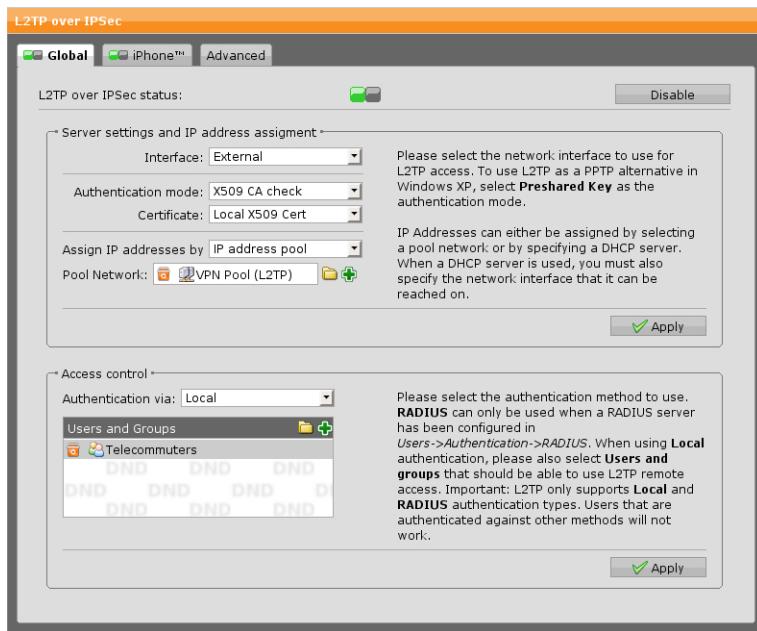


Figure 16.8 Configuring L2TP Remote Access

The status icon turns amber and the *Server Settings and IP Address Assignment* area becomes editable.

2. Make the following settings:

Interface: Select the network interface to be used for L2TP VPN access.

Authentication Mode: You can choose between the following authentication modes:

- **Preshared Key:** Enter a password which is subsequently used as pre-shared key. The *Preshared Key* method makes use of a shared secret that is exchanged by the communicating parties prior to the communication taking place. To communicate, both parties prove that they know the secret. The shared secret is a secure phrase or password that is used to encrypt the traffic using the encryption algorithm for L2TP. For best security, you should take appropriate measures to increase the strength of the shared secret. The security of a shared secret depends on the quality of the password and how securely it has been transmitted. Passwords consisting of common words are extremely vulnerable to dictionary attacks. For that reason, the shared secret should be quite

long and contain a variety of letters, capital letters, and numbers. Consequently, using a preshared secret as an authentication method should be replaced by certificates whenever possible.

Note – If you want to enable access for iPhones you need to select *Pre-shared Key* because iPhones only support PSK authentication.

- **X.509 CA Check:** X.509 certificates ease the process of exchanging public authentication keys in large VPN setups with a lot of participants. A so-called *Certification Authority (CA)* gathers and checks the public keys of the VPN endpoints and issues a certificate for each member. The certificate contains the peer's identity along with its public key. Because the certificate is digitally signed, no one else can issue a forged certificate without being detected.

During the key exchange, certificates are exchanged and verified using locally stored CA public keys. The actual authentication of the VPN endpoints is then done by using public and private keys. If you want to use this authentication mode, select an X.509 certificate.

Note that for X.509 authentication to work, you need to have a valid CA configured on the *Remote Access >> Certificate Management >> Certificate Authority* tab.

Assign IP Addresses By: You can use this function to define whether an address from a defined VPN pool shall be assigned during the dial-up or whether the address will be automatically requested from a DHCP server.

- **Pool Network:** By default, *IP Address Pool* is selected as IP address assignment, having the pre-defined *VPN Pool (L2TP)* network definition selected as the *Pool Network*. The *VPN Pool (L2TP)* is a randomly generated network from the 10.x.x.x IP address space for private internets, using a class C subnet. It is normally not necessary to ever change this, as it ensures that the users have a dedicated pool of addresses to make connections from. If you want to use a different network, you can simply change the definition of the *VPN Pool (L2TP)*, or assign another network as IP address pool here.

Note – If you use private IP addresses for your L2TP VPN Pool and you want IPSec hosts to be allowed to access the Internet, appropriate masquerading or NAT rules must be in place for the IP address pool.

- **DHCP Server:** If you select *DHCP Server*, also specify the network interface through which the DHCP server is connected. The DHCP server does not have to be directly connected to the interface—it can also be accessed through a router. Note that the local DHCP server is not supported; the DHCP server selected here must be running on a physically different system.

3. Click **Apply**.

Your settings will be saved.

To cancel the configuration, click *Abort* or the amber colored status icon.

Access Control

Authentication Via: L2TP remote access only supports local and RADIUS authentication.

- **Local:** If you select *Local*, specify the users and user groups who should be able to use L2TP remote access. It is not possible to drag backend user groups into the field. For local users you need to add users in the usual way and enable L2TP for them. If no users or groups are selected, L2TP remote access is turned off.

Note – Similar to SSL VPN the *Remote Access* menu of the User Portal can only be accessed by users who are selected in the *Users and Groups* box and for whom a user definition does exist on the security system. Otherwise the User Portal will display the note "Unfortunately this remote access method is not configured for you" on the *Remote Access >> L2TP VPN* tab. Depending on the authentication mode, authorized users who have successfully logged in to the User Portal will find the IPSec pre-shared key (authentication mode *Preshared key*) or the PKCS#12 file (authentication mode *X.509 CA check*) as well as a link to installation instructions, which are available at the Astaro knowledgebase³⁹ (navigate to *ASG Version 7 >> Remote Access >> L2TP over IPSec*).

-
- **RADIUS:** If you select *RADIUS*, the authentication requests are forwarded to the RADIUS server. The L2TP module sends the "l2tp" string as NAS-ID

³⁹ <http://www.astaro.com/kb>

to the RADIUS server.

The authentication algorithm gets automatically negotiated between client and server. For local users, Astaro Security Gateway supports the following authentication protocols:

- MSCHAPv2
- PAP

By default, a Windows client negotiates MSCHAPv2.

For RADIUS users, Astaro Security Gateway supports the following authentication protocols:

- MSCHAPv2
- MSCHAP
- CHAP
- PAP

iPhone

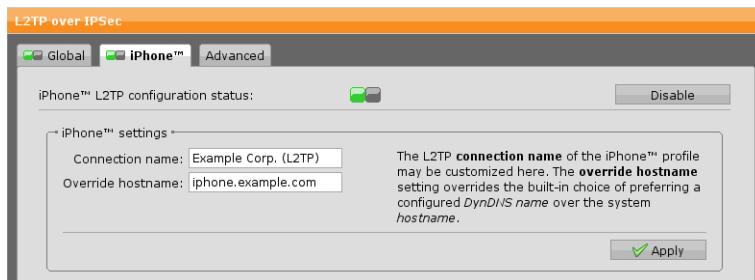


Figure 16.9 Configuring iPhone Remote Access Via L2TP Over IPSec

You can enable that iPhone users are offered automatic L2TP over IPSec configuration in the User Portal.

However, only users that have been added to the *Users and Groups* box on the *Global* tab will find configuration files on their User Portal site. The iPhone status is enabled by default.

Connection Name: Enter a descriptive name for the L2TP over IPSec connection so that iPhone users may identify the connection they are going to establish. The default name is your company name followed by the protocol L2TP over IPSec.

Note – Connection Name must be unique among all iPhone connection settings (PPTP, L2TP over IPSec, Cisco VPN Client).

Override Hostname: In case the system hostname cannot be publicly resolved by the client, you can enter a server hostname here that overrides the internal preference of the *DynDNS Hostname* before the *System DNS Hostname*.

To disable automatic iPhone configuration, click the status icon or *Disable* in the header of the tab.

The status icon turns red.

Advanced

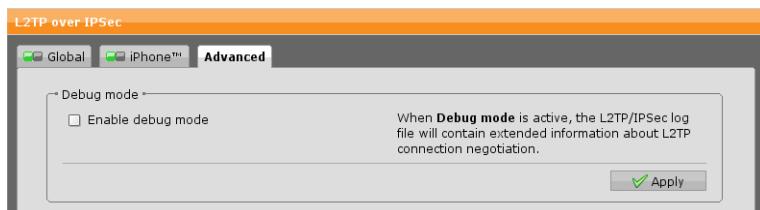


Figure 16.10 Configuring Advanced L2TP Remote Access Settings

Debug Mode

Enable Debug Mode: This option controls how much debug output is generated in the L2TP over IPSec log. Select this option if you encounter connection problems and need detailed information about the negotiation of client parameters, for example.

IPSec

IP Security (IPSec) is a standard for securing *Internet Protocol* (IP) communications by encrypting and/or authenticating all IP packets.

The IPSec standard defines two service modes and two protocols:

- Transport mode
- Tunnel mode
- *Authentication Header (AH)* authentication protocol
- *Encapsulated Security Payload (ESP)* encryption (and authentication) protocol

IPSec also offers methods for manual and automatic management of *Security Associations* (SAs) as well as key distribution. These characteristics are consolidated in a *Domain of Interpretation (DOI)*.

IPSec Modes

IPSec can work in either transport mode or tunnel mode. In principle, a host-to-host connection can use either mode. If, however, one of the endpoints is a security gateway, the tunnel mode must be used. The IPSec VPN connections on this security system always use the tunnel mode.

In transport mode, the original IP packet is not encapsulated in another packet. The original IP header is retained, and the rest of the packet is sent either in clear text (AH) or encrypted (ESP). Either the complete packet can be authenticated with AH, or the payload can be encrypted and authenticated using ESP. In both cases, the original header is sent over the WAN in clear text.

In tunnel mode, the complete packet—header and payload—is encapsulated in a new IP packet. An IP header is added to the IP packet, with the destination address set to the receiving tunnel endpoint. The IP addresses of the encapsulated packets remain unchanged. The original packet is then authenticated with AH or encrypted and authenticated using ESP.

IPSec Protocols

IPSec uses two protocols to communicate securely on the IP level.

- **Authentication Header (AH):** A protocol for the authentication of packet senders and for ensuring the integrity of packet data.
- **Encapsulating Security Payload (ESP):** A protocol for encrypting the entire packet and for the authentication of its contents.

The *Authentication Header* protocol (AH) checks the authenticity and integrity of packet data. In addition, it checks that the sender and receiver IP addresses have not been changed in transmission. Packets are authenticated using a checksum created using a *Hash-based Message Authentication Code* (HMAC) in connection with a key. One of the following hashing algorithms will be used:

- **Message Digest Version 5 (MD5):** This algorithm generates a 128-bit checksum from a message of any size. This checksum is like a fingerprint of the message, and will change if the message is altered. This hash value is sometimes also called a digital signature or a message digest.
- **The Secure Hash (SHA-1):** This algorithm generates a hash similar to that of MD5, though the SHA-1 hash is 160 bits long. SHA-1 is more secure than MD5, due to its longer key.

Compared to MD5, an SHA-1 hash is somewhat harder to compute, and requires more CPU time to generate. The computation speed depends, of course, on the processor speed and the number of IPSec VPN connections in use at the Astaro Security Gateway.

In addition to encryption, the *Encapsulated Security Payload* protocol (ESP) offers the ability to authenticate senders and verify packet contents. If ESP is used in tunnel mode, the complete IP packet (header and payload) is encrypted. New, unencrypted IP and ESP headers are added to the encapsulating packet: The new IP header contains the address of the receiving gateway and the address of the sending gateway. These IP addresses are those of the VPN tunnel.

For ESP with encryption normally the following algorithms are used:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Of these, AES offers the highest standard of security. The effective key lengths that can be used with AES are 128, 192 and 256 bits. Astaro Security Gateway supports a number of encryption algorithms. Either the MD5 or SHA-1 algorithms can be used for authentication.

NAT Traversal (NAT-T)

NAT traversal is a technology for establishing connections between hosts in TCP/IP networks which use NAT devices. This is achieved by using UDP encapsulation of the ESP packets to establish IPSec tunnels through NAT devices. UDP encapsulation is only used if NAT is detected between the IPSec peers; otherwise normal ESP packets will be used.

With NAT traversal you are able to place the firewall or a road warrior behind a NAT router and still establish an IPSec tunnel. Both IPSec peers must support NAT traversal if you want to use this feature, which is automatically negotiated. Make sure that the NAT device has IPSec-passthrough turned off, because this could impair the use of NAT traversal.

If road warriors want to use NAT traversal, their corresponding user object in WebAdmin must have a static remote access IP address (RAS address) set (see also *Use Static Remote Access IP* on the user definitions page in WebAdmin).

By default, a NAT traversal keep-alive signal is sent at intervals of 60 seconds to prevent an established tunnel from expiring when no data is transmitted. The keep-alive messages are sent to ensure that the NAT router keeps the state information associated with the session so that the tunnel stays open.

Connections

On the *IPSec >> Connections* tab you can create and edit IPSec connections.

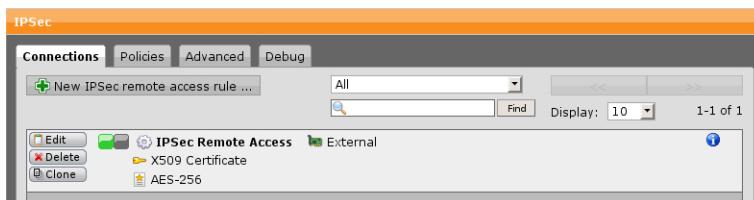


Figure 16.11 Configuring IPSec Remote Access

To create an IPSec connection, proceed as follows:

1. On the **Connections** tab, click **New IPSec Remote Access Rule**.

The *Add IPSec Remote Access Rule* dialog box opens.

2. Make the following settings:

Name: Enter a descriptive name for this connection.

Interface: Select the name of the interface which is used as the local endpoint of the IPSec tunnel.

Local Networks: Select the local networks that should be reachable through the VPN tunnel.

Policy: Select the IPSec policy for this IPSec connection. IPSec policies can be defined on the *Remote Access >> IPSec >> Policies* tab.

Authentication Type: Select the authentication type for this remote gateway definition. The following types are available:

- **Preshared key:** Authentication with *Preshared Keys* (PSK) uses secret passwords as keys. These passwords must be distributed to the endpoints before establishing the connection. When a new VPN tunnel is established, each side checks that the other knows the secret password. The security of PSKs depends on the quality of the passwords used: common words and phrases are subject to dictionary attacks. Permanent or long-term IPSec connections should use certificates instead.
- **X.509 Certificate:** The X.509 Certificate authentication scheme uses public keys and private keys. An X.509 certificate contains the public key together with information identifying the owner of the key. Such certificates are signed and issued by a trusted *Certificate Authority* (CA). Once selected, specify the users that should be allowed to use this IPSec connection. It is not possible to drag backend user groups into the *Allowed Users* field. Unless you select the checkbox *Automatic Packet Filter Rules*, you need to specify appropriate packet filter rules manually in the *Network Security* menu.

Note – The User Portal can only be accessed by users who are selected in the *Allowed Users* box and for whom a user definition does exist on the security system. Authorized users who have successfully logged in to the User Portal will find the *Astaro Secure Client* (ASC), its configuration file, the PKCS#12 file as well as a link to installation instructions, which are available at the Astaro knowledgebase⁴⁰ (navigate to *ASG Version 7 >> Remote Access >> IPSec*).

- **CA DN Match:** This authentication type uses a match of the *Distinguished Name* (DN) of CA certificates to verify the keys of the VPN endpoints. Once selected, select an *Authority* and choose a *DN Mask* that matches the DNs of remote access clients. Now select or add a *Peer Subnet Range*. Clients are only allowed to connect if the DN mask matches the one in their certificate.

Enable XAUTH (optional): Extended authentication should be enabled to require authentication of users against configured backends.

Automatic Packet Filter Rules (optional): This option is only available with the authentication type *X.509 Certificate*.

Once the IPSec connection has been successfully established, packet filter

⁴⁰ <http://www.astaro.com/kb>

rules will automatically be added for the respective data traffic. They will be removed as soon as the connection is closed.

Comment (optional): Add a description or other information about the IPSec connection.

3. Click Save.

The new remote access rule appears on the *Connections* list.

To either edit or delete a remote access rule, click the corresponding buttons.

Policies

On the *Remote Access >> IPSec >> Policies* tab you can customize parameters for IPSec connections and unite them into a policy. An IPSec policy defines IKE (Internet Key Exchange) and IPSec proposal parameters of an IPSec connection. Note that each IPSec connection needs an IPSec policy.

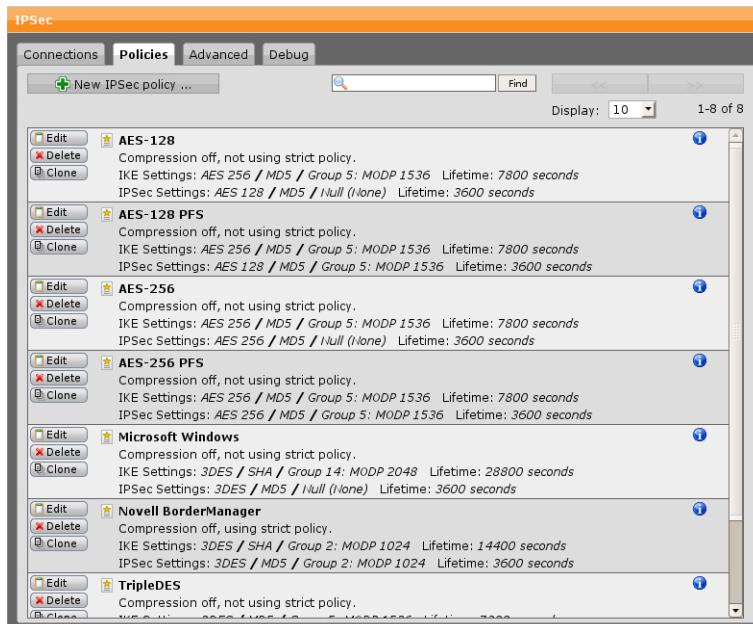


Figure 16.12 IPSec Policies List

To create an IPSec policy, proceed as follows:

1. **On the Policy tab, click New IPSec Policy.**

The Add IPSec Policy dialog box opens.

2. **Make the following settings:**

Name: Enter a descriptive name for this policy.

IKE Encryption Algorithm: The encryption algorithm specifies the algorithm used for encrypting the IKE messages. Supported algorithms are:

- o *DES* (56 bit)
- o *3DES* (168 bit)
- o *AES 128* (128 bit)
- o *AES 192* (192 bit)
- o *AES 256* (256 bit)
- o *Blowfish* (128 bit)
- o *Twofish* (128 bit)
- o *Serpent* (128 bit)

IKE Authentication Algorithm: The authentication algorithm specifies the algorithm used for integrity checking of the IKE messages. Supported algorithms are:

- o *MD5* (128 bit)
- o *SHA* (160 bit)
- o *SHA 256* (256 bit)
- o *SHA 512* (512 bit)

IKE SA Lifetime: This value specifies the timeframe in seconds for which the IKE SA is valid and when the next rekeying should take place. Valid values are between 60 sec and 28800 sec (8 hrs). The default value is 7800 seconds.

IKE DH Group: When negotiating a connection, the communicating parties also settle the actual keys used to encrypt the data. In order to generate a session key, IKE uses the *Diffie-Hellman* (DH) algorithm, which utilizes random data. The random data generation is based on pool bits. The IKE group basically tells the number of pool bits. The more pool bits, the larger the random numbers. The larger the numbers, the harder it is to crack the

Diffie-Hellman algorithm. As a consequence, more pool bits mean more security but also the consumption of more CPU resources. Currently, the following Diffie-Hellman groups are supported:

- Group 1: MODP 768
 - Group 2: MODP 1024
 - Group 5: MODP 1536
 - Group 14: MODP 2048
 - Group 15: MODP 3072
 - Group 16: MODP 4096
-

Note – Group 1 (MODP 768) is considered weak and only supported for interoperability reasons.

IPSec Encryption Algorithm: The same encryption algorithms as for IKE.

IPSec Authentication Algorithm: The same authentication algorithms as for IKE.

IPSec SA Lifetime: This value specifies the timeframe in seconds for which the IPSec SA is valid and when the next rekeying should take place. Valid values are between 60 sec and 86400 sec (1 day). The default value is 7800 seconds.

IPSec PFS Group: *Perfect Forward Secrecy* (PFS) refers to the notion that if a session key is compromised, it will permit access only to data of this specific session. In order for PFS to exist, the key used to protect the IPSec SA must not be derived from random keying material used to get the keys for the IKE SA. Therefore, PFS initiates a second Diffie-Hellman key exchange proposing the selected DH group for the IPSec connection to get a new randomly generated key. Supported Diffie-Hellman groups are the same as for IKE.

Enabling PFS is considered to be more secure, but it takes also more time for the exchange. It is not recommended to use PFS on slow hardware.

Note – PFS is not fully interoperable with all vendors. If you notice problems during the negotiation, you might consider disabling PFS.

Strict Policy: If an IPSec gateway makes a proposition with respect to an encryption algorithm and to the strength, it might happen that the gateway of the receiver accepts this proposition, even though the IPSec policy does not correspond to it. If you select this option and the remote endpoint does not agree on using exactly the parameters you specified, the IPSec connection will not be established. Suppose the IPSec policy of your security system requires AES-256 encryption, whereas, for example, a road warrior with SSH Sentinel wants to connect with AES-128; with the strict policy option enabled, the connection would be rejected.

Note – The compression setting will not be enforced via *Strict Policy*.

Compression: This option specifies whether IP packets should be compressed by means of the *IP Payload Compression Protocol* (IPComp) prior to encryption. IPComp reduces the size of IP packets by compressing them to increase the overall communication performance between a pair of communicating hosts or gateways. Compression is turned off by default.

Comment (optional): Add a description or other information about the policy.

3. Click **Save**.

The new policy appears on the *Policies* list.

To either edit or delete a policy, click the corresponding buttons.

Advanced

On the *Site-to-site VPN >> IPSec >> Advanced* tab you can configure advanced options of IPSec VPN. Depending on your preferred authentication type, you can define the local certificate (for X.509 authentication) and the local RSA key (for RSA authentication), among other things. Note that this should only be done by experienced users.

Local X.509 Certificate

With X.509 authentication, certificates are used to verify the public keys of the VPN endpoints. If you want to use this authentication type, you have to select a local certificate from the drop-down list in the *Local X.509 Certificate* area. The selected key/certificate is then used to authenticate the firewall to remote peers if X.509 authentication is selected.

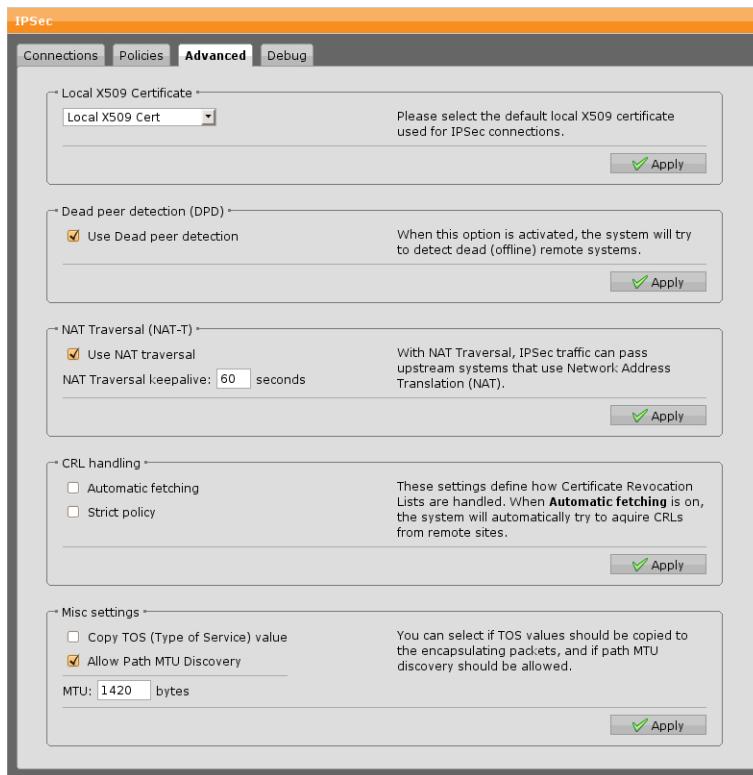


Figure 16.13 Configuring Advanced IPSec Remote Access Settings

You can only select certificates where the appropriate private key is present, other certificates are not available in the drop-down list.

If there is no certificate available for selection, you have to add one in the *Certitificate Management* menu, either by creating a new one or by importing one using the upload function.

After selecting the certificate, enter the passphrase the private key was protected with. During the saving process, the passphrase is verified and an error message is displayed if it does not match the encrypted key.

Once an active key/certificate is selected, it is displayed in the *Local X.509 Certificate* area.

Dead Peer Detection (DPD)

Use Dead Peer Detection: The dead peer detection option is used for automatically terminating a connection if the remote VPN gateway or client is unreachable. For connections with static endpoints, the tunnel will be re-negotiated

automatically. Connections with dynamic endpoints require the remote side to re-negotiate the tunnel. Usually it is safe to always enable this option. The IPSec peers automatically determine whether the remote side supports dead peer detection or not, and will fall back to normal mode if necessary.

NAT Traversal (NAT-T)

Use NAT Traversal: Select to enable that IPSec traffic can pass upstream systems which use *Network Address Translation* (NAT). Additionally, you can define the keepalive interval for NAT traversal. Click *Apply* to save your settings.

CRL Handling

Automatic Fetching: There might be situations in which the provider of a certificate attempts to revoke the confirmation awarded with still valid certificates, for example if it has become known that the receiver of the certificate fraudulently obtained it by using wrong data (name, etc.) or because an attacker has got hold of the private key, which is part of the certified public key. For this purpose, so-called *Certificate Revocation Lists* or CRLs are used. They normally contain the serial numbers of those certificates of a certifying instance, that have been held invalid and that are still valid according to their respective periods of validity.

After the expiration of these periods the certificate will no longer be valid and must therefore not be maintained in the block list. The *Automatic CRL Fetching* function automatically requests the CRL through the URL defined in the partner certificate via HTTP, Anonymous FTP or LDAP version 3. On request, the CRL can be downloaded, saved and updated, once the validity period has expired. If you use this feature, make sure that you set the packet filter rules accordingly, so that the CRL distribution server can be accessed.

Strict Policy: If this option is enabled, any partner certificate without a corresponding CRL will be rejected.

Misc Settings

Copy TOS Flag: Type of Service bits (TOS bits) are several four-bit flags in the IP header. These bits are referred to as *Type of Service* bits because they allow the transferring application to tell the network which type of service quality is necessary. The following service types are available:

- Minimize delay (binary number: 1000)
- Maximize throughput (binary number: 0100)
- Maximize reliability (binary number: 0010)
- Minimize monetary cost (binary number: 0001)
- Normal service (binary number: 0000)

Enabling this option will copy the content of the *Type of Service* field into the encrypted data packet, so that the IPSec data traffic can be routed according to its priority.

Allow Path MTU Discovery: It is usually preferable that IP data packets be of the largest size that does not require fragmentation anywhere along the path from the source to the destination. This size of the data packet is referred to as the *Path Maximum Transmission Unit* (PMTU). If any of the data packets are too large to be forwarded without fragmentation by some router along the path, that router will discard them and return *ICMP Destination Unreachable* messages with a code meaning "fragmentation needed and DF set". Upon receipt of such a message, the source host reduces its assumed PMTU for the path.

MTU: In this field you can specify the *Maximum Transmission Unit* (MTU) of the IPSec interface; the default MTU is 1420 byte.

Debug

On the *Debug* tab you can configure IKE debug options. Select the checkboxes for which types of IKE messages you want to create debug output. The following flags can be logged:

- **Control:** Displays control messages of IKE state
- **Emitting:** Displays content of outgoing IKE messages
- **Parsing:** Displays content of incoming IKE messages
- **Raw:** Displays messages as raw bytes
- **Crypt:** Shows encryption and decryption operations

Cisco VPN Client

Astaro Security Gateway supports IPSec remote access via Cisco VPN Client. The Cisco VPN Client is an executable program from Cisco Systems that allows computers to connect remotely to a *Virtual Private Network* (VPN) in a secure way.

Global

On the *Remote Access >> Cisco VPN Client >> Global* tab you can configure basic options for setting up remote access via Cisco VPN Client.

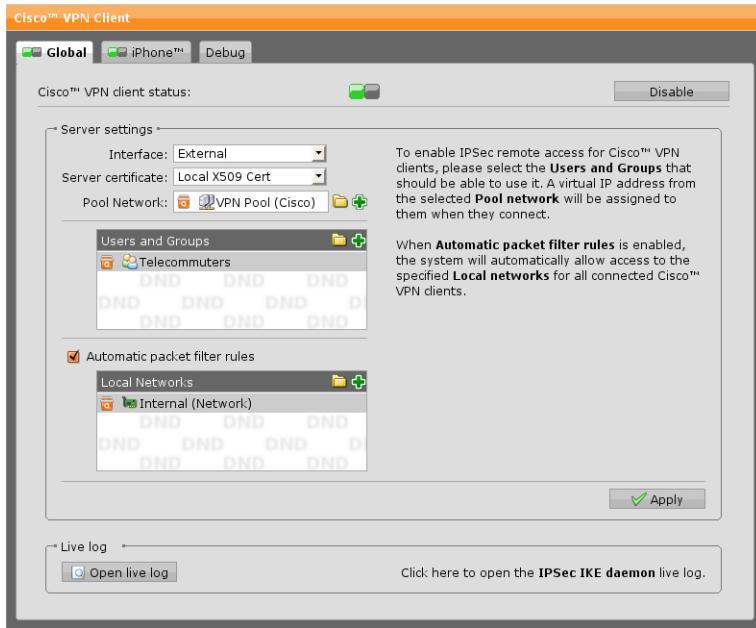


Figure 16.14 Configuring Remote Access Via Cisco VPN Client

To configure Astaro Security Gateway to allow Cisco VPN Client connections, proceed as follows:

1. **On the *Global* tab enable Cisco VPN Client.**

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *Server Settings* area becomes editable.

2. **Make the following settings:**

Interface: Select an interface to be used for Cisco VPN Client connections.

Server Certificate: Select the certificate with which the server identifies itself to the client.

Pool Network: Select a network pool to choose virtual network addresses from to assign them to connecting clients. By default *VPN Pool (Cisco)* is selected.

Users and Groups: Select users and/or groups that are allowed to connect to the security system via Cisco VPN Client. However, it is not possible to drag backend membership groups into the box because a user certificate is needed at IPSec configuration time but the *certificate* is only generated when a user successfully logs in for the first time.

Automatic Packet Filter Rules (optional): Select this checkbox to automatically create packet filter rules that grant access to (below) specified local networks. If you do not select this checkbox or create packet filter rules yourself clients are blocked by the firewall.

Local Networks: Select local networks here for which the automatic packet filter rules are applied. Users connecting to the security system via Cisco VPN Client are allowed to access them.

3. Click **Apply**.

Your settings will be saved.

Live Log

Use the live log to track connection logs of the IPSec IKE daemon log. It shows information on establishing, upkeeping, and closing connections.

iPhone

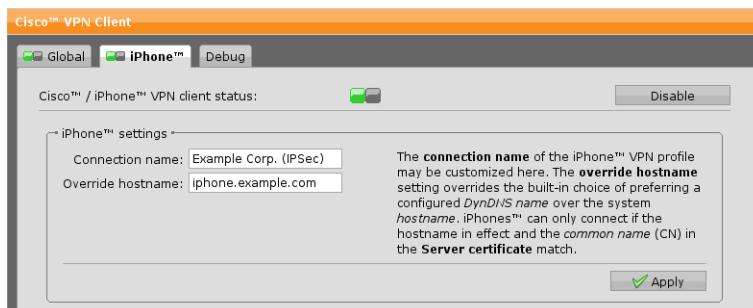


Figure 16.15 Configuring iPhone Remote Access Via Cisco VPN Client

You can enable that iPhone users are offered automatic Cisco IPSec configuration in the User Portal.

However, only users that have been added to the *Users and Groups* box on the *Global* tab will find configuration files on their User Portal site. The iPhone status is enabled by default.

Connection Name: Enter a descriptive name for the Cisco IPSec connection so that iPhone users may identify the connection they are going to establish. The default name is your company name followed by the protocol Cisco IPSec.

Note – Connection Name must be unique among all iPhone connection settings (PPTP, L2TP over IPSec, Cisco VPN Client).

Override Hostname: In case the system hostname cannot be publicly resolved by the client, you can enter a server hostname here that overrides the internal preference of the *DynDNS Hostname* before the *System DNS Hostname*.

To disable automatic iPhone configuration, click the status icon or *Disable* in the header of the tab.

The status icon turns red.

Note that connecting iPhones get presented the server certificate specified on the *Global* tab. The iPhone checks whether the VPN ID of this certificate corresponds to the server hostname and refuses to connect if they differ. If the server certificate uses *Distinguished Name* as VPN ID Type it compares the server hostname with the *Common Name* field instead. You need to make sure the server certificate fulfills these constraints.

Debug

On the *Debug* tab you can configure IKE debug options. Select the checkboxes for which types of IKE messages you want to create debug output. The following flags can be logged:

- **Control:** Displays control messages of IKE state
- **Emitting:** Displays content of outgoing IKE messages
- **Parsing:** Displays content of incoming IKE messages
- **Raw:** Displays messages as raw bytes
- **Crypt:** Shows encryption and decryption operations

Advanced

On the *Remote Access >> Advanced* page you can make the advanced configurations for remote access clients. The IP addresses of the DNS and WINS servers you enter here are provided for the use of remote access clients while establishing a connection to the firewall, thus providing full name resolution for your domain.

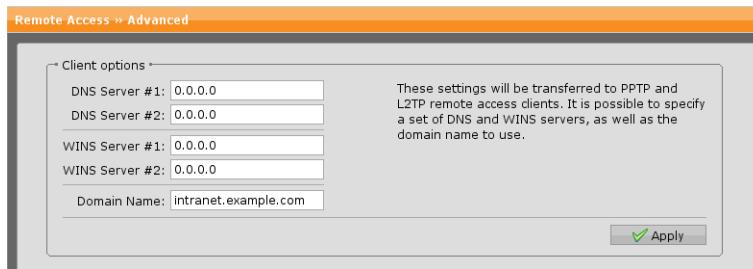


Figure 16.16 Configuring Advanced Remote Access Settings

DNS Server: Specify up to two DNS servers of your organization.

WINS Server: Specify up to two WINS servers of your organization.

Windows Internet Naming Service (WINS) is Microsoft's implementation of *NetBIOS Name Server (NBNS)* on Windows operating systems. Effectively, WINS is to NetBIOS names what DNS is to domain names—a central mapping of hostnames to IP addresses.

Domain Name: Enter the *fully qualified domain name* (FQDN) of your organization. The fully qualified domain name is an unambiguous domain name that specifies the node's absolute position in the DNS tree hierarchy, for example `intranet.example.com`.

Note – The domain name can only be automatically distributed to the remote access client during connection initiation using SSL. For IPSec, on the other hand, the domain name will be written to the Astaro Secure Client's configuration file, which must be imported into the client by hand. However, for PPTP and L2TP over IPSec the domain name *cannot* be distributed automatically, but needs to be configured on the client side.

Certificate Management

Using the *Remote Access >> Certificate Management* menu, which contains the same configuration options as the *Site-to-site VPN >> Certificate Management* menu, you can manage all certificate-related operations of Astaro Security Gateway. This includes creating or importing X.509 certificates as well as uploading so-called *Certificate Revocation List* (CRL), among other things.

Certificates

See *Site-to-site VPN >> Certificate Management >> Certificates*.

Certificate Authority

See *Site-to-site VPN >> Certificate Management >> Certificate Authority.*

Revocation Lists

See *Site-to-site VPN >> Certificate Management >> Revocation Lists.*

Advanced

See *Site-to-site VPN >> Certificate Management >> Advanced.*

Logging

This chapter describes how to configure the logging capabilities of Astaro Security Gateway.

Astaro Security Gateway provides extensive logging capabilities by continuously recording various system and network protection events. The detailed audit trail provides both historical and current analysis of various network activities to help identify potential security threats or to troubleshoot occurring problems.

The *Log Partition Status* page in WebAdmin shows the status of the log partition of your Astaro Security Gateway unit, including information about the disk space left and fillup rate as well as a four-week histogram of the log partition utilization. As the fillup rate is the difference between the measurement point and the starting point divided by the time elapsed, the value is somewhat inaccurate in the beginning but becomes more precise the longer the system is up.

The following topics are included in this chapter:

- Settings
- Viewing of log files

Settings

In the *Logging >> Settings* menu you can configure basic settings for local and remote logging.

Local Logging

On the *Logging >> Settings >> Local Logging* tab you can make the settings for local logging. Local logging is enabled by default. However, to activate local logging in case it was disabled, proceed as follows:

1. **On the *Local Logging* tab enable local logging.**

You can either click the status icon or the *Enable* button.

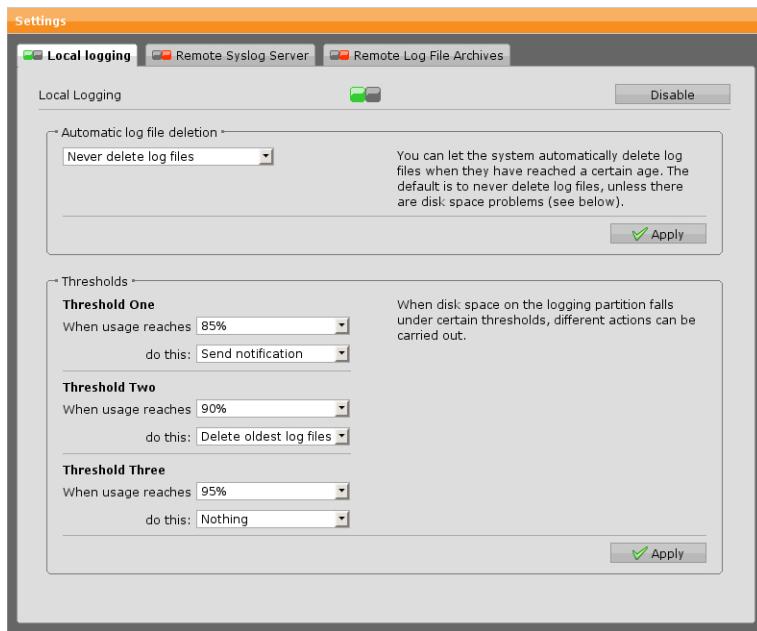


Figure 17.1 Configuring Local Logging Settings

The status icon turns green and the *Automatic Log File Deletion* area becomes editable.

2. **Select a time frame when log files are to be deleted.**
From the drop-down list select what action is to be applied automatically on log files. *Never delete log files* is selected by default.
3. **Click *Apply*.**
Your settings will be saved.

Thresholds

Here you can define thresholds for local logging which are bound to certain actions that are to be carried out if a threshold is reached. You can select among the following actions:

- **Nothing:** No actions will be initiated.
- **Send Notification:** A notification will be sent to the administrator stating that the threshold was reached.

- **Delete Oldest Logfiles:** Oldest log files will be deleted until the remaining amount is below the configured threshold or until the log file archive is empty. In addition, a notification of that event will be sent to the administrator.
- **Shutdown System:** The system will be shut down. A notification of that event will be sent to the administrator.

In case of a system shutdown, the administrator has to change the configuration of the local logging, configure log file deletion or move away/delete log files manually. If the reason for the system shutdown persists, the system will shut down itself again the next time the log cleaning process runs, which happens daily at 12:00 AM (i.e., at midnight).

Click *Apply* to save your settings.

Remote Syslog Server

On the *Logging >> Settings >> Remote Syslog Server* tab you can make the settings for remote logging. This function allows you to forward log messages from the firewall to other hosts. This is especially useful for networks using a host to collect logging information from several firewalls. The selected host must run a logging daemon that is compatible to the Syslog protocol.

To configure a remote syslog server, proceed as follows:

1. **On the *Remote Syslog Server* tab enable remote syslog.**
You can either click the status icon or the *Enable* button.
The status icon turns amber and the *Remote Syslog Settings* area becomes editable.
2. **Click the plus icon in the *Syslog Servers* box to create a server.**
The Add Syslog Server dialog box opens.
3. **Make the following settings:**
Name: Enter a descriptive name for the remote syslog server.
Server: Add or select the host that should receive log data from the firewall.

Caution – Do not use one of the firewall's own interfaces as a remote syslog host, since this will result in a logging loop.

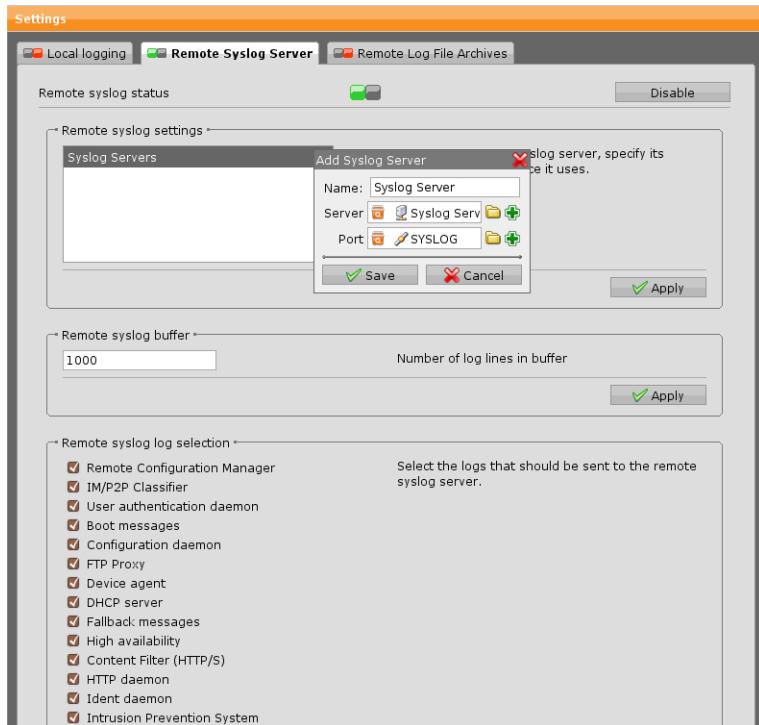


Figure 17.2 Configuring a Remote Syslog Server

Port: Add or select port which is to be used for the connection.

4. **Click *Apply*.**

Your settings will be saved.

Remote Syslog Buffer

In this area you can change the buffer size of the remote syslog. The buffer size is the number of log lines kept in the buffer. Default is 1000. Click *Apply* to save your settings.

Remote Syslog Log Selection

This area is only editable when remote syslog is enabled. Select the checkboxes of the logs that should be delivered to the syslog server. Click *Apply* to save your settings.

Remote Logfile Archives

On the *Logging >> Settings >> Remote Logfile Archives* tab you can make the settings for remote archiving of log files. If remote log file archiving is enabled, the log files of the past day are packed and compressed into one file, which is transferred to a remote log file storage. Using the drop-down list you can select your preferred transfer method.

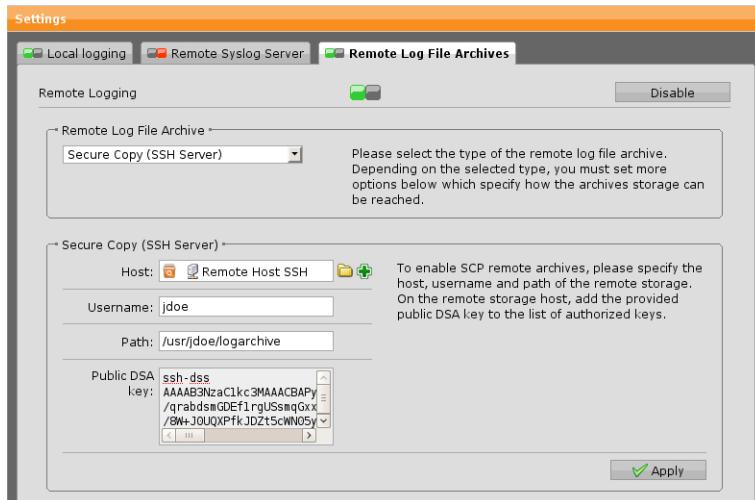


Figure 17.3 Configuring Remote Log File Archiving

To configure a remote log file archive, proceed as follows:

1. **Enable the *Remote Log File Archives* function.**

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *Remote Logfile Archive* area becomes editable.

2. **Select the logfile archiving method.**

From the drop-down list, select your preferred archiving method. Depending on your selection, the related configuration options for each archiving method will be displayed below. You can choose between the following archiving methods:

- **FTP Server:** The *File Transfer Protocol* (FTP) method needs the following parameters to be set:

- *Host*: Host definition of the FTP server.
 - *Service*: TCP port the server is listening on.
 - *Username*: Username for the FTP server account.
 - *Password*: Password for the FTP server account.
 - *Path*: Remote (relative) path where the log files are stored.
- **SMB (CIF Share)**: The SMB method needs the following parameters to be set:
 - *Host*: Host definition of the SMB server.
 - *Username*: Username for the SMB account.
 - *Password*: Password for the SMB account.

Security Note – The password will be saved plain-text in the configuration file. It is therefore advisable to create a user/password combination uniquely for this logging purpose.

- *Share*: SMB share name. Enter the path or the network share information where the log files are to be transferred to, e.g. /logs/logfile_archive.
 - *Workgroup/Domain*: Enter the workgroup or domain the log file archive is part of.
- **Secure Copy (SSH Server)**: To use the SCP method, it is necessary that you add the public SSH DSA key to the authorized keys of your SCP server. On a Linux system, you can simply cut and paste the SSH DSA key and add it to the `~/.ssh/authorized_keys` file of the configured user account. During the installation, Astaro Security Gateway creates a new SSH DSA key. For security reasons, this SSH DSA key is not included in backups. After a new installation or the installation of a backup, you must therefore store the new SSH DSA key on the remote server to be able to securely copy your logfile archives to the SCP server. The SCP method requires the following settings:

- **Host:** Host definition for the SCP server.
 - **Username:** Username for the SCP server account.
 - **Path:** Remote (full) path where the log files should be stored.
 - **Public DSA Key:** On the remote storage host, add the provided public DSA key to the list of authorized keys.
- **Send by E-mail:** To have the logfile archive sent by e-mail, enter a valid e-mail address.

3. Click **Apply**.

Your settings will be saved.

If the transfer fails, the archive will remain on the firewall. During each run of the log cleaning process, the firewall tries to deliver all remaining archives.

View Log Files

The *Logging >> View Log Files* menu offers the possibility to view different kind of log files and to search in log files.

Today's Log Files

On the *Logging >> View Log Files >> Today's Logfiles* tab all current logs can easily be accessed.

Log name	Activity	Size	Actions
<input type="checkbox"/> Admin notifications	Today	5.5 kB	[Live Log] [View] [Clear]
<input type="checkbox"/> Boot messages			[Live Log]
<input type="checkbox"/> Configuration daemon	Now	1.0 MB	[Live Log] [View] [Clear]
<input type="checkbox"/> Content Filter (HTTP)	Today	103 kB	[Live Log] [View] [Clear]
<input type="checkbox"/> DHCP server			[Live Log]
<input type="checkbox"/> DNS proxy	Today	13.8 kB	[Live Log] [View] [Clear]
<input type="checkbox"/> Device agent			[Live Log]

Figure 17.4 View Today's Log Files

This tab provides various actions that can be applied to all log files. The following actions are available:

- **Live Log:** Opens a pop-up windows allowing you to view the logfile in real-time. New lines are added to the logfile on the fly. If you select *Autoscroll*, the pop-up window will automatically scroll down to always display the most recent log. In addition, the pop-up window also contains a filter text box that allows you to limit the display of new logs to only those records that match the filter.
- **View:** Opens a pop-up windows that shows the logfile in its current state.
- **Clear:** Deletes the contents of the logfile.

Using the drop-down list in the table footer, you can either download selected log files as a **zip** file or clear their contents simultaneously.

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7. The Live Log pop-up might stop adding lines in some cases. If you experience this kind of problem, try to press F5 (refresh) within the Live Log window.

Archived Log Files

On the *Logging >> View Log Files >> Archived Log Files* tab you can manage the log file archive. All log files are archived on a daily basis. To access an archived log file, select the subsystem of Astaro Security Gateway for which logs are written as well as a year and month.

All available log files that match your selection will be displayed in chronological order. You can either view the archived logfile or download it in **zip** file format.

Using the drop-down list in the table footer, you can either download selected log files as a **zip** file or delete them simultaneously.

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

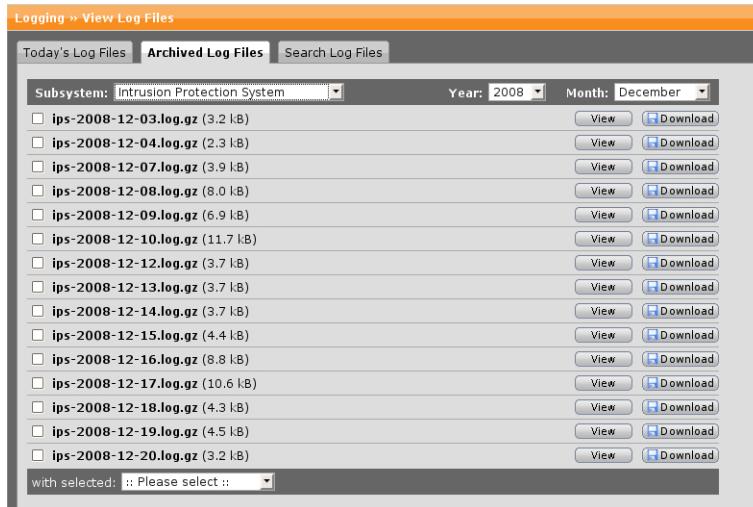


Figure 17.5 Selecting Archived Log Files

Search Log Files

The tab *Logging >> View Log Files >> Search Log Files* enables you to search through your local log files for various time periods. First, select the log file you want to search through, then enter the search term and select the time range. If you select *Custom time frame* from the *Time Frame* list, you can specify a start and end date. After clicking the *Start Search* button, a popup window will open presenting the results of your query. Depending on your browser it may be necessary to allow pop-up windows for WebAdmin.

The screenshot shows the 'Search Log Files' tab interface. It includes a descriptive text block, input fields for selecting the log file, search term, and time frame, and dropdown menus for custom start and end dates. A 'Start search' button is located at the bottom right.

Query log files

You can search log files with this form. Select the subsystem, a timeframe and enter a text string to search for. A popup window will open that contains the results. You can open several windows at the same time.

Select log file to search:

Search term:

Select time frame:

Custom start date:

Custom end date:

Figure 17.6 Searching Log Files

Reporting

The reporting function of Astaro Security Gateway provides real-time information by collecting current log data and presenting it in a graphical format.

The following topics are included in this chapter:

- Settings
- Hardware
- Network Usage
- Network Security
- Web Security
- Mail Security
- Executive Report

Settings

In the *Reporting >> Settings* menu you can make settings for the reporting functions such as enabling/disabling certain features of reporting, setting time frames and amounts for keeping data. Additionally, you can anonymize data to enhance privacy protection.

Settings

The *Settings* tab allows you to define reporting actions and the time period reporting data will be kept on the system before it is automatically deleted. The following report topics can be set:

- Accounting
- Authentication
- Mail Security

- IM/P2P
- IPS
- Packet Filter
- Web Security

Use the checkboxes on the left side to enable or disable reporting for a certain report topic. By default, all report topics are enabled.

Use the drop-down lists on the right to determine how long reporting data is kept.

Note – Disabling needless reports will lower the base load of your machine and can reduce performance bottlenecks. Try to keep time frames as short as possible since high amounts of stored data result in a higher base load and decreased responsiveness on the dynamical reporting pages.

The settings on this tab do not affect the log file archives.

Executive Report Settings

In this area you can define respectively the number of executive reports to keep:

- Daily reports: 60 at maximum
- Weekly reports: 52 at maximum
- Monthly reports: 12 at maximum

Click *Apply* to save your settings.

For more information on the executive report and its options, see *Reporting >> Executive Report*.

PDF Paper Settings

The default paper format for the PDF executive report is A4. Using the drop-down list you can alternatively select *Letter* or *Legal*. Click *Apply* to save your settings.

Exceptions

The *Settings >> Exceptions* tab allows you to exclude certain domains and addresses from reporting, which affects the Executive Report as well as the

respective *Reporting* sections. You can define exceptions for the following reports:

- Web Security: domains
- Mail Security: domains and addresses
- Network Security: IP addresses

Define exceptions in the respective boxes and click *Apply*. Note the import function with which you can define multiple items at once.

Anonymizing

The *Settings >> Anonymizing* tab allows to anonymize data based on the four-eyes principle. That means that deanonymization can only take place when two different people agree on that procedure.

Anonymization ensures that user data is kept secret when viewing logging and reporting data, and therefore actions (such as web-surfing habits) cannot be traced back to a specific person.

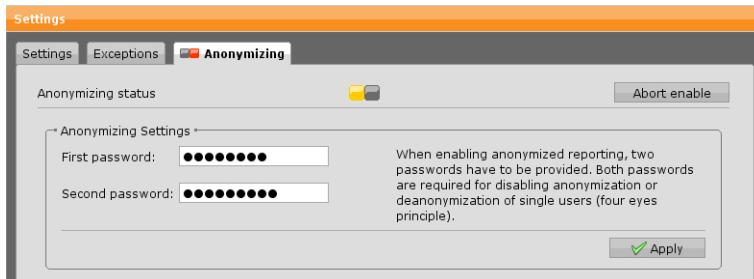


Figure 18.1 Enabling Anonymization of User Data

To use anonymization, proceed as follows:

1. **On the *Anonymizing* tab enable anonymization.**

You can either click the status icon or the *Enable* button.

The status icon turns amber and the *Anonymizing Settings* area becomes editable.

2. **Enter two security passwords.**

The four-eyes principle is only allowed for when two different people enter a password unknown to each other.

3. **Click *Apply*.**

Your settings will be saved.

To disable anonymization (globally) again, both passwords are necessary.

1. **On the Anonymizing tab click Disable or the status icon.**

The status icon turns amber and the *Anonymizing Settings* area becomes editable.

2. **Enter both passwords.**

Enter the first and the second password that have been provided to enable anonymization.

3. **Click Apply.**

Your settings will be saved.

If necessary, anonymization can be disabled for single users, see *Reporting >> Web Security* and *Reporting >> Mail Security*.

Hardware

The tabs of the *Reporting >> Hardware* menu provide overview statistics about the utilization of hardware components for several time periods.

Daily

The *Hardware >> Daily* tab provides overview statistics about the following hardware components of the last 24 hours:

- CPU Usage
- Memory/Swap Usage
- Partition Usage

CPU Usage: Processor utilization in percent.

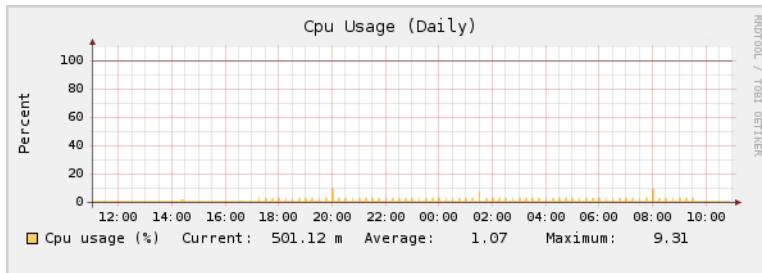


Figure 18.2 Histogram of the CPU Utilization

Memory/Swap Usage: The utilization of memory and swap in percent. The swap usage heavily depends on your system configuration. The activation of system services such as Intrusion Prevention or the proxy servers will result in a higher memory usage. If the system runs out of free memory, it will begin to use swap space, which decreases the overall performance of the system. The used swap space should be as low as possible. To achieve that, increase the total amount of memory available to your system.

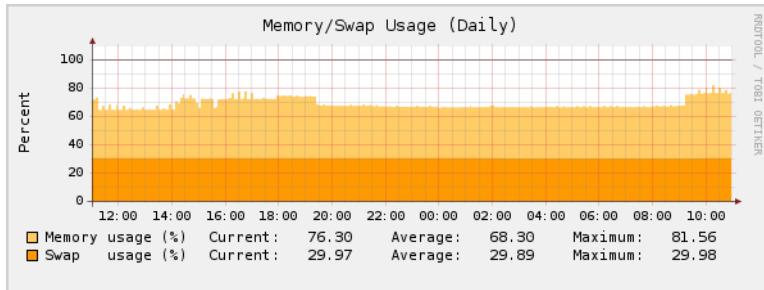


Figure 18.3 Histogram of the Memory/Swap Utilization

Partition Usage: The utilization of selected partitions in percent. All charts show three graphs, each representing one hard disk drive partition:

- **Root:** The root partition is the partition where the root directory of Asaro Security Gateway is located. In addition, this partition stores update packages and backups.
- **Log:** The log partition is the partition where log files and reporting data is stored. If you run out of space on this partition, please adjust your settings under *Logging >> Settings >> Local Logging*.
- **Storage:** The storage partition is the partition where proxy services store their data, for example images for the HTTP proxy, messages for the SMTP proxy, quarantined mails and the like.

Weekly

The *Hardware >> Weekly* tab provides overview statistics about selected hardware components for the last seven days. For more information, see *Daily*.

Monthly

The *Hardware >> Monthly* tab provides overview statistics about selected hardware components for the last four weeks. For more information, see *Daily*.

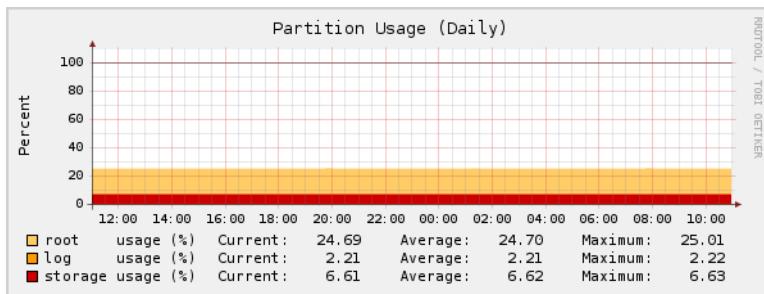


Figure 18.4 Histogram of the Partition Utilization

Yearly

The *Hardware >> Yearly* tab provides overview statistics about selected hardware components for the last twelve months. For more information, see *Daily*.

Network Usage

The tabs of the *Reporting >> Network Usage* menu provide overview statistics about the traffic passing each interface of Astaro Security Gateway for several time periods. Each chart presents its data using the following units of measurement:

- u (Micro, 10^{-6})
- m (Milli, 10^{-3})
- k (Kilo, 10^3)
- M (Mega, 10^6)
- G (Giga, 10^9)

Note that the scaling can range from 10^{-18} to 10^8 .

Daily

The *Network Usage >> Daily* tab provides overview statistics about the traffic passing each configured interface of the last 24 hours.

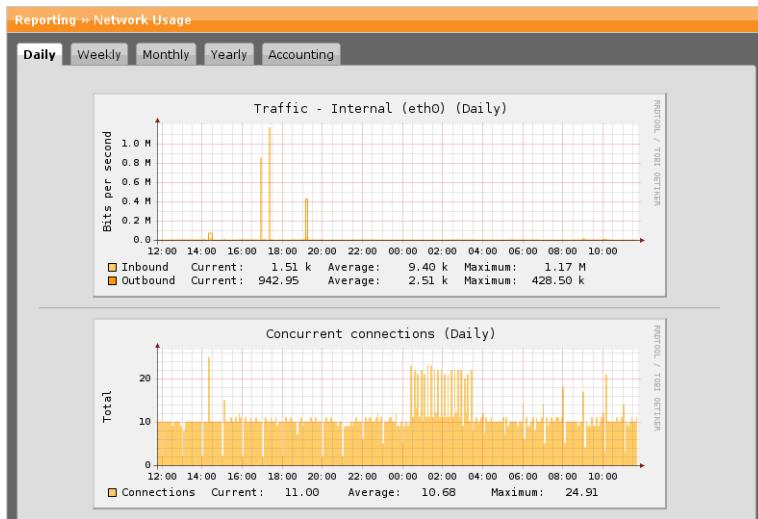


Figure 18.5 Histogram of the Ethernet Interfaces Utilization

Each histogram shows two graphs:

- **Inbound:** The average incoming traffic for that interface, in bits per second.
- **Outbound:** The average outgoing traffic for that interface, in bits per second.

The *Concurrent Connections* chart shows you the total of concurrent connections.

Weekly

The *Network Usage >> Weekly* tab provides overview statistics about the traffic passing each configured interface of the last seven days. For more information, see *Daily*.

Monthly

The *Network Usage >> Monthly* tab provides overview statistics about the traffic passing each configured interface of the last four weeks. For more information, see *Daily*.

Yearly

The *Network Usage >> Yearly* tab provides overview statistics about the traffic passing each configured interface of the last twelve months. For more information, see *Daily*.

Accounting

The *Network Usage >> Accounting* tab presents comprehensive data about the network traffic which was transferred to/from and through the device.

Top	Service	Protocol	IN	%	OUT	%	Total	%	Conn	%
1	WEBADMIN	TCP	7.3 MB	29.91%	35.8 MB	66.87%	43.2 MB	55.25%	2 078	20.39%
2	SSH	TCP	3.7 MB	15.07%	11.0 MB	20.60%	14.7 MB	18.86%	9	0.09%
3	0	ICMP	5.9 MB	23.87%	5.7 MB	10.57%	11.5 MB	14.75%	21	0.21%
4	BOOTPS	UDP	5.2 MB	21.34%	0	0.00%	5.2 MB	6.71%	1 876	18.41%
5	SMTP	TCP	1.5 MB	6.14%	68.3 KB	0.12%	1.6 MB	2.02%	21	0.21%
6	HTTPS	TCP	299.4 KB	1.19%	491.8 KB	0.90%	791.2 KB	0.99%	439	4.31%
7	DOMAIN	UDP	253.1 KB	1.01%	506.2 KB	0.92%	759.3 KB	0.95%	3 791	37.20%
8	NETBIOS-DGM	UDP	318.6 KB	1.27%	0	0.00%	318.6 KB	0.40%	1 328	13.03%
9	NETBIOS-NS	UDP	36.9 KB	0.15%	0	0.00%	36.9 KB	0.05%	484	4.75%
10	NTP	UDP	14.5 KB	0.06%	14.5 KB	0.03%	28.9 KB	0.04%	143	1.40%
Totals			24.6 MB		53.6 MB		78.1 MB		10 190	

Figure 18.6 Accounting Data Sorted for Top Services

If an IP or a hostname is clicked in the result table on the *By Client/By Server* views, it will automatically be used as a filter for the *Top Services By Client* view. You can change this afterwards to the *Top Services by Server* view, or manually provide an IP/Network, as well as network ranges (e.g., 192.168.1.0/24 or 10/8), and use those settings by using the *Update* button. On the *By Service* views you can enter protocol and service, separated by comma (e.g., *TCP,SMTP, UDP,6000*). If you do not supply the protocol, TCP will be assumed (e.g. *HTTP* is also valid).

If there are more than 20 results per page, you can jump forward and backward using the next page and previous page buttons, respectively.

For your convenience, accounting data can be downloaded in PDF or Excel format by clicking one of the corresponding buttons in the top right corner of the *Accounting* tab. The report is generated from the current view you have selected.

Please note that the labels *IN* and *OUT* for traffic may vary depending on the point of view. When running in proxy mode, the client connects to port 8080 on the ASG (even in transparent mode), so data sent by the client (the request) is seen as *incoming* traffic and the data sent to the client (the response) is seen as *outgoing* traffic on the internal interface.

Tip – You can sort all data by clicking the table column headings. For example, if you want to sort all hosts by incoming traffic, click on *IN* in the table heading. Thus, hosts causing the most incoming traffic will be listed first. Note that the data for traffic is given in kibibytes (KiB) and mebibytes (MiB), both of which are base-2 units of computer storage (e.g., 1 kibibyte = 2^{10} bytes = 1 024 bytes).

Network Security

The tabs of the *Reporting >> Network Security* menu provide overview statistics about relevant network security events detected by Astaro Security Gateway.

Daily

The *Network Security >> Daily* tab provides overview statistics about the following events of the last 24 hours:

- Packet Filter Violations
- Intrusion Prevention Events

Packet Filter Violations: Every data packet that is dropped or rejected is counted as a packet filter violation. The number of packet filter violations is calculated over a time span of five minutes.

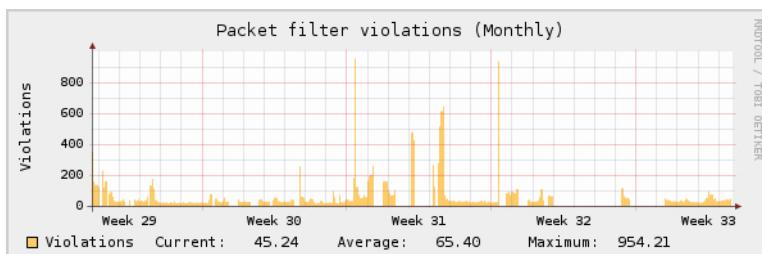


Figure 18.7 Histogram of Packet Filter Violations (Monthly)

Intrusion Prevention Events: All charts show two graphs:

- **Alert Events:** The number of data packets that triggered an intrusion alert.
- **Drop Events:** The number of data packets that were dropped by the intrusion prevention system.

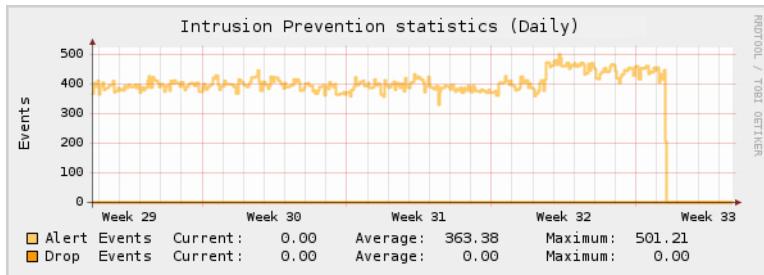


Figure 18.8 Histogram of Intrusion Prevention Events (Monthly)

Weekly

The *Network Security >> Weekly* tab provides overview statistics about packet filter violations and intrusion prevention events of the last seven days. For more information, see *Daily*.

Monthly

The *Network Security >> Monthly* tab provides overview statistics about packet filter violations and intrusion prevention events of the last four weeks. For more information, see *Daily*.

Yearly

The *Network Security >> Yearly* tab provides overview statistics about packet filter violations and intrusion prevention events of the last twelve months. For more information, see *Daily*.

Packet Filter

The *Network Security >> Packet Filter* tab presents comprehensive data about the packet filter activity, classified according to source IP, source hosts, number of received packets and number of services.

If you click an IP or a hostname in the result table, it will automatically be used as a filter for the *Top Services* view. You can manually provide an IP/Network, as well as network ranges (e.g., 192.168.1.0/24 or 10/8), and use those settings by using the *Update* button.

On the *By Service* views you can enter protocol and service, separated by comma (e.g., *TCP,SMTP, UDP,6000*).

If there are more than 20 results per page, you can jump forward and backward using the next page and previous page buttons, respectively.

For your convenience, packet filter data can be downloaded in PDF or Excel format by clicking one of the corresponding buttons in the top right corner of the *Packet Filter* tab. The report is generated from the current view you have selected.

Tip – You can sort all data by clicking the table column headings. For example, if you want to sort the table by number of services, click on *Services* in the table heading. Thus, the source IP having requested the most services is listed first.

IPS

The *Network Security >> IPS* tab presents comprehensive data about intrusion prevention activities on your network.

For your convenience, IPS data can be downloaded in PDF or Excel format by clicking one of the corresponding buttons in the top right corner of the *IPS* tab. The report is generated from the current view you have selected.

Tip – You can sort all data by clicking the table column headings. For example, if you want to sort the table by number of packets, click on *Packets* in the table heading. Thus, the source IP having requested the most packets is listed first.

Web Security

The tabs of the *Reporting >> Web Security* menu provide overview statistics about the most active web users and most frequently visited websites.

Web Usage

The *Web Security >> Web Usage* tab contains comprehensive statistics about the most active web users and most frequently visited domains given for various time ranges. Always confirm your changes by clicking the *Update* button. If there are more than 20 results per page, you can jump forward and backward using the next page and previous page buttons, respectively.

For your convenience, usage data can be downloaded in PDF or Excel format by clicking one of the corresponding buttons in the top right corner of the *Web Usage* tab. The report is generated from the current view you have selected.

Tip – You can sort all data by clicking the table column headings. For example, if you want to sort all users by traffic, click on *Traffic* in the table heading. Thus, users causing the most traffic will be listed first. Note that the data for traffic is given in kibibytes (KiB) and mebibytes (MiB), both of which are base-2 units of computer storage (e.g., 1 kibibyte = 2^{10} bytes = 1 024 bytes).

The most active web users do not appear immediately in the table, but only after a session timeout had occurred. This is the case if a certain client (username or IP address) has ceased to surf the web for five minutes. The security system determines this surfing session as "dead" and sends it to a database before it gets displayed on the most active web users list.

In addition, you can also select *Top Users By Domain* or *Top Domains By User*. If you select *Top Users By Domain*, type the domain you want to search for into the *Domain* box, then confirm your settings by clicking *Update*.

Note that you can use the percent sign (%) as a wildcard. For example, by placing a percent sign at the end of your keyword, you are telling Astaro Security Gateway to look for exact matches or sub-sets. So if your search was "example%", the following would all return as hits: example.com, example.net, example.org.

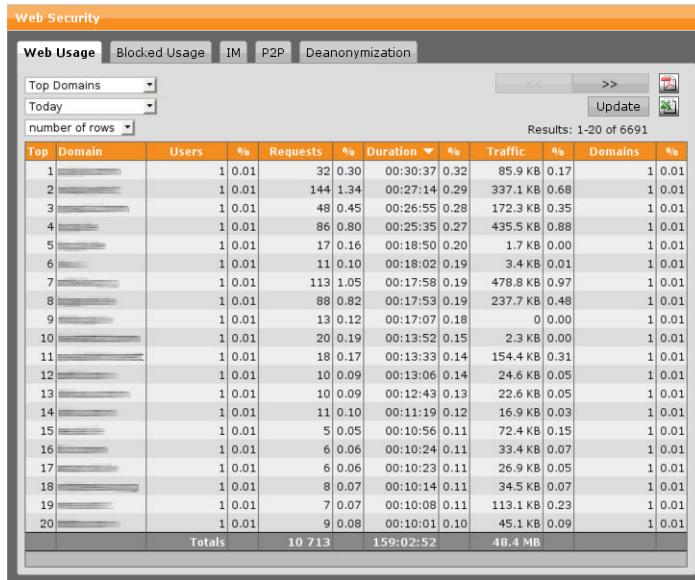


Figure 18.9 Ranking of Top Domains

If you select *Top Domains By User*, enter the IP address you want to search for into the *User* box, then confirm your settings by clicking *Update*. Here, too, you can use the percent sign as a wildcard.

Note on error domains – When clients try to request invalid URLs, the proxy will log the request but will not be able to serve it. Those links will be counted with *error* as domain. This is not an error of the reporting or the HTTP/S proxy; in most cases, those errors occur because invalid or malformed links are placed in web content by the page creator.

Blocked Usage

The *Web Security >> Blocked Usage* tab contains comprehensive statistics about all blocked web requests based on surf protection and antivirus. Always confirm your changes by clicking the *Update* button. If there are more than 20 results per page, you can jump forward and backward using the next page and previous page buttons, respectively.

For your convenience, usage data can be downloaded in PDF or Excel format by clicking one of the corresponding buttons in the top right corner of the *Blocked Usage* tab. The report is generated from the current view you have selected.

IM

The *Web Security >> IM* tab presents comprehensive data about instant messaging activities on your network.

For your convenience, IM data can be downloaded in PDF or Excel format by clicking one of the corresponding buttons in the top right corner of the *IM* tab. The report is generated from the current view you have selected.

Tip – You can sort all data by clicking the table column headings. For example, if you want to sort the table by number of packets, click on *Packets* in the table heading. Thus, the source IP having requested the most packets is listed first.

P2P

The *Web Security >> P2P* tab presents comprehensive data about peer-to-peer activities on your network.

For your convenience, P2P data can be downloaded in PDF or Excel format by clicking one of the corresponding buttons in the top right corner of the *P2P* tab. The report is generated from the current view you have selected.

Tip – You can sort all data by clicking the table column headings. For example, if you want to sort the table by number of packets, click on *Packets* in the table heading. Thus, the source IP having requested the most packets is listed first.

Deanonymization

The *Web Security >> Deanonymization* tab is only accessible if anonymization is activated (see *Reporting >> Settings >> Anonymizing*).

Here it is possible to abandon anonymization for specific users regarding web security reports. Proceed as follows:

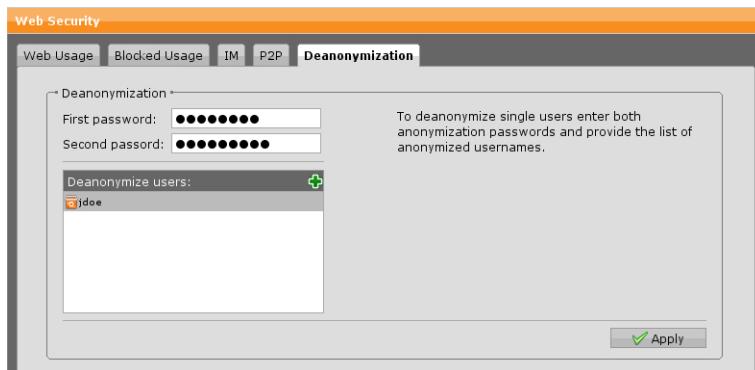


Figure 18.10 Deanonymizing Single Users

1. Enter both passwords.

Enter the first and the second password that have been provided to enable anonymization.

2. Add users to deanonymize.

To the *Deanonymize Users* box add the usernames of those users you want to deanonymize.

3. Click *Apply*.

Your settings will be saved.

Mail Security

The tabs of the *Reporting >> Mail Security* menu provide overview statistics about mail flow, mail usage and mail security.

Usage Graphs

The *Mail Security >> Usage Graphs* tab provides overview statistics about the mail flow on the ASG given for various time frames:

- Daily
- Weekly
- Monthly
- Yearly

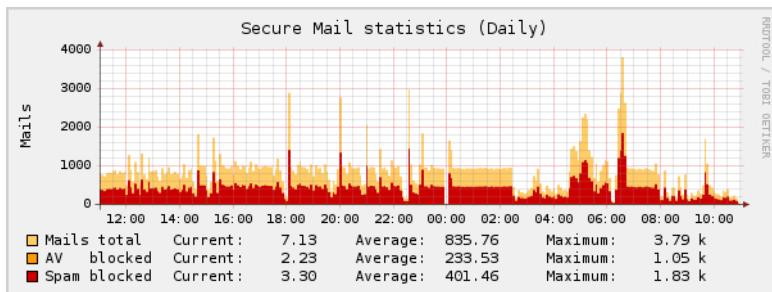


Figure 18.11 Histogramm of the Mail Flow

Mail Usage

The *Mail Security >> Mail Usage* tab contains comprehensive statistics about the most actively used e-mail addresses and address domains given for various time ranges. Always confirm your changes by clicking the *Update* button. If there are more than 20 results per page, you can jump forward and backward using the next page and previous page buttons, respectively.

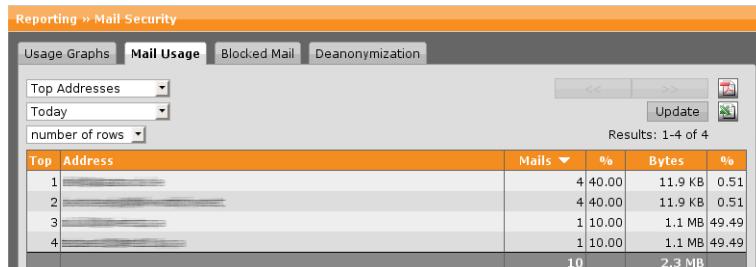


Figure 18.12 Ranking of Most Active E-mail Addresses

Blocked Mail

The *Mail Security >> Blocked Mail* tab contains comprehensive statistics about all blocked e-mail requests based on antivirus and antispam. Always confirm your changes by clicking the *Update* button. If there are more than 20 results per page, you can jump forward and backward using the next page and previous page buttons, respectively.

Deanonymization

The *Mail Security >> Deanonymization* tab is only accessible if anonymization is activated (see *Reporting >> Settings >> Anonymizing*).

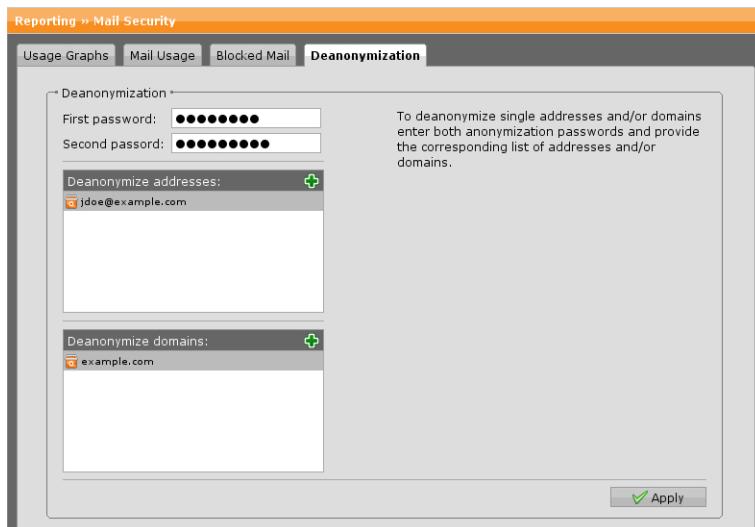


Figure 18.13 Deanonymizing E-mail Addresses and Domains

Here it is possible to abandon anonymization for specific e-mail addresses and/or domains regarding mail security reports. Proceed as follows:

1. Enter both passwords.

Enter the first and the second password that have been provided to enable anonymization.

2. Make the following settings:

Deanonymize Addresses: You can add e-mail addresses you want to deanonymize.

Deanonymize Domains: You can add domains you want to deanonymize.

3. Click *Apply*.

Your settings will be saved.

Provided e-mail addresses and domains become readable in reports.

Executive Report

In the menu *Reporting >> Executive Report* you can create a collection of the most important reporting data presented in graphical format to show network utilization for a number of services.

View Report

On the *Reporting >> Executive Report >> View Report* tab you can create a complete executive report based on the individual reports in the tabs and pages of the *Reporting* menu. Click the button *Generate Report Now* to open a window showing the executive report.

Archived Executive Reports

The *Executive Report >> Archived Executive Reports* tab provides an overview of all archived executive reports. Only those executive reports will be archived for which archiving has been selected on the *Configuration* tab.

Configuration

On the *Executive Report >> Configuration* tab you can make the settings for executive reports.

Select the time period for the executive report. The report can be created on a daily, weekly, or monthly basis. If you select *Weekly*, you can additionally choose the weekday when the executive report should start to collect its data.

In addition, enter the e-mail addresses of the recipients who should receive the executive report. Note that for various time periods different e-mail addresses can be configured.

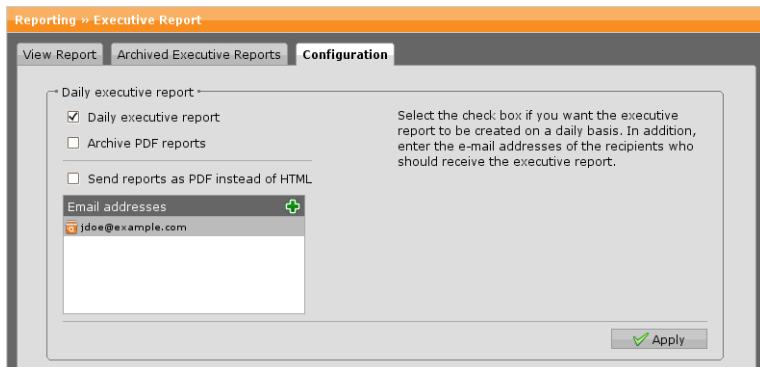


Figure 18.14 Configuration of the Daily Executive Report

Support

This chapter describes the support tools available for Astaro Security Gateway. The pages of the *Support* menu contain many customer support related features ranging from various web links, through contact information, to the output of useful network tools that are used to determine important network properties without the need to access the firewall's command-line interface.

The following topics are included in this chapter:

- Manual
- Contact Support
- Tools
- Advanced

In addition, the main page of the *Support* menu contains web links to the following information resources:

- **Knowledgebase:** Astaro's official knowledgebase containing numerous information on configuring Astaro Security Gateway.
- **Known Issue List:** The list of known problems that cannot be fixed or for which a workaround is available.
- **Hardware Compatibility List:** The list of hardware that is compatible to Astaro Security Gateway Software.
- **Up2Date Information:** Astaro's Up2Date blog, which informs about product improvements and firmware updates.

Manual

On the *Support >> Manual* page you can download the current Administration Guide in PDF format. Select the language of the guide and click *Download*. Note that you need a special reader to open PDF documents such as Adobe's Reader or Xpdf.

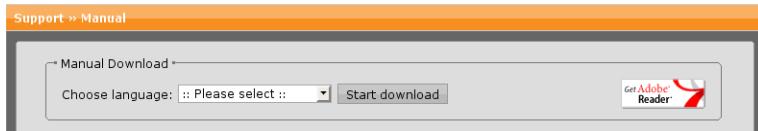


Figure 19.1 Downloading the Administration Guide of Astaro Security Gateway

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

Contact Support

Astaro offers a comprehensive range of customer support services for its security solutions. Based on the support/maintenance level, you have various levels of access and committed response time by the Astaro service department and/or Astaro's certified partners.

All support cases concerning Astaro Security Gateway are processed via the Astaro Partner Portal⁴¹. You may open a support case via a web form by clicking *Open Support Case*.

⁴¹ https://www.astaro.com/license/support_cases

Tools

The tabs of the *Support >> Tools* menu display the output of useful network tools that can be used to determine important network properties without the need to access the firewall's command-line interface. The output of the following tools can be viewed:

- Ping
- Traceroute
- DNS Lookup

Ping Check

The program *ping* is a computer network tool used to test whether a particular host is reachable across an IP network. Ping works by sending ICMP *echo request* packets to the target host and listening for ICMP *echo response* replies. Using interval timing and response rate, ping estimates the round-trip time and packet loss rate between hosts.

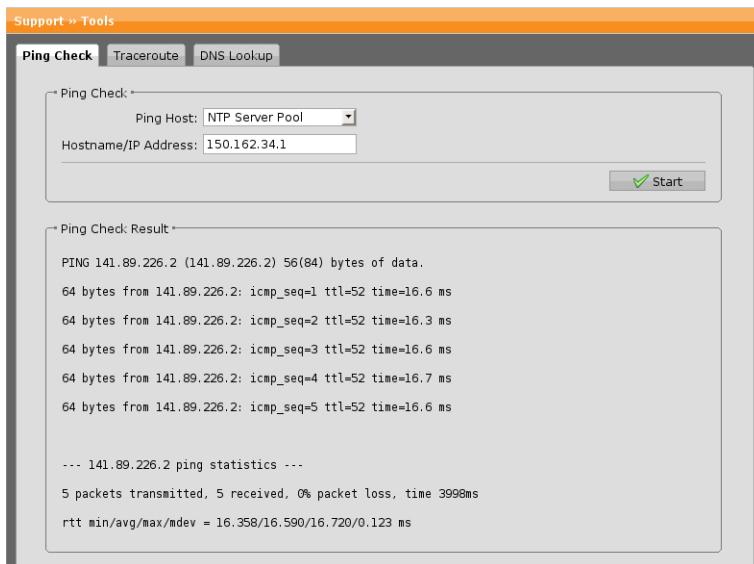


Figure 19.2 Checking the Availability of an Host Using Ping

To make a ping check, proceed as follows:

1. Select the ping host.

Select the host you want to ping. In the *Ping Host* box, you can select a host for which a host definition exists. Alternatively, you can also enter a custom hostname or IP address.

2. Click **Start**.

The output of the ping check will be displayed in the *Ping Check Result* area.

Traceroute

The program *traceroute* is a computer network tool used to determine the route taken by packets across an IP network. It lists the IP addresses of the routers that were involved in transporting the packet. If the packet's route cannot be determined within a certain time frame, traceroute will report an asterisk (*) instead of the IP address. After a certain number of failures, the check will end. An interruption of the check can have many causes, but most likely it is caused by a packet filter along the network path that blocks traceroute packets.

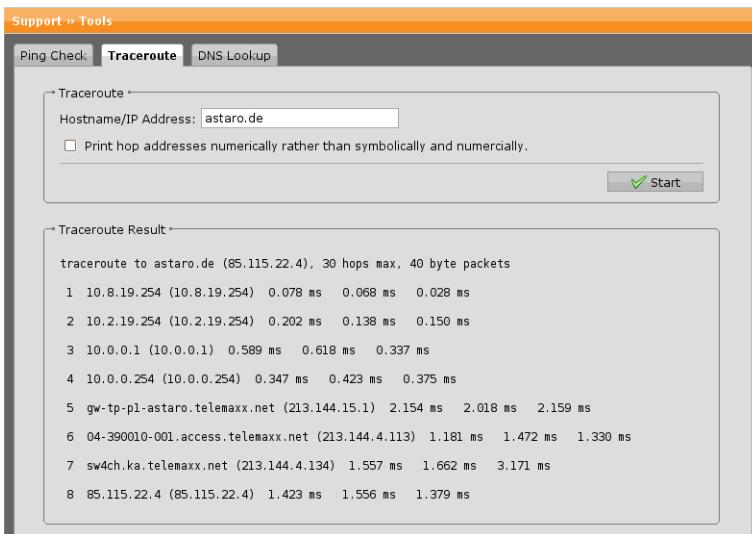


Figure 19.3 Checking a Route Using Traceroute

To trace a route, proceed as follows:

1. Specify the hostname/IP address.

Enter the hostname or IP address of the host for which you want to determine the route.

2. Print hop addresses numerically (optional).

Selecting this option saves a nameserver address-to-name lookup for each gateway found on the path.

3. Click *Start*.

The output of traceroute will be displayed in the *Traceroute Result* area.

DNS Lookup

The program *dig* (short for *Domain Information Groper*) is a network tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

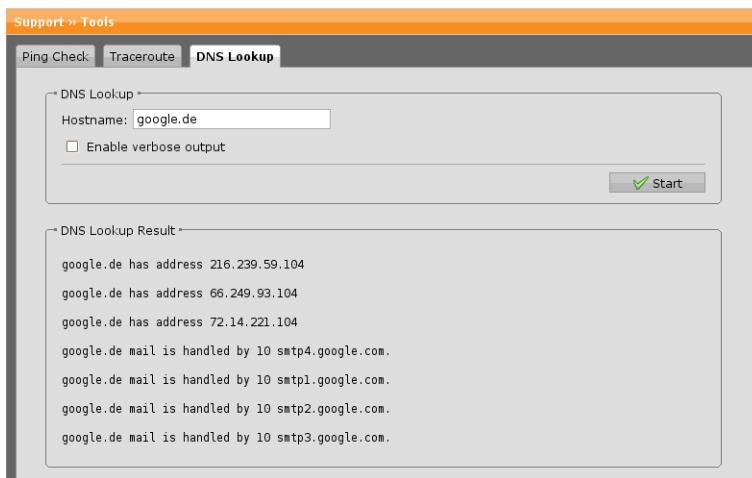


Figure 19.4 Looking up an DNS Entry Using Dig

To make a DNS lookup, proceed as follows:

1. Specify the hostname/IP address.

Enter the hostname or IP address of the host for which you want to determine DNS information.

2. Select *Enable Verbose Output* (optional).

Select this option to generate lengthy output showing more information.

3. Click *Start*.

The output of dig will be displayed in the *DNS Lookup Result* area.

Advanced

The *Support >> Advanced* tabs display even more information on your firewall such as its process status, among others.

Process List

The program *ps* displays a header line followed by lines containing information about your processes that have controlling terminals. This information is sorted by controlling terminal, then by process ID.

Local Network Connections

The program *netstat* (short for *Network Statistics*) is a network tool that displays a list of the active Internet connections a computer currently has, both incoming and outgoing.

Routes Table

The program *ip* is a network tool for controlling TCP/IP networking and traffic control. Invoked with the parameter `route show table all` it displays the contents of all routing tables of the firewall.

Interfaces Table

The table shows all configured interfaces of Astaro Security Gateway, both network interface cards and virtual interfaces. The program *ip* invoked with parameter `addr` displays interfaces and their properties.

Config Dump

For debugging or recovery purposes it is useful to gather as many information as possible about your installation of Astaro Security Gateway. The support package that can be downloaded from the *Support >> Advanced >> Configuration Dump* tab provides exactly this. The zip file contains the following items:

- The entire dump of the firewall's configuration (`storage.abf`). Note that this is no genuine backup file—it does not contain any passwords, among other things—and can be used for debugging purposes only.
 - Information on the hardware present in the system (`hwinfo`).
 - Information on the software packages installed on the system (`swinfo`).
-

Note – To avoid problems with file downloads using Internet Explorer 6, add the URL of the firewall (e.g., <https://192.168.2.100>) and the User Portal (e.g., <https://192.168.2.100>) to the Trusted Sites, which are configured in IE's *Internet Options >> Security*. In addition, select *Automatic Prompting for File Downloads* in the *Trusted Sites Zone* when using Internet Explorer 7.

Resolve REF

For debugging purposes you can resolve configuration references internally used by the system. If you encounter a reference somewhere in the logs, you can paste the reference string here (e.g., `REF_DefaultSuperAdmin`). WebAdmin will then display an excerpt of the configuration daemon's data structure.

Appendix A

Glossary

ACPI

The Advanced Configuration and Power Interface (ACPI) specification is a power management standard that allows the operating system to control the amount of power distributed to the computer's devices.

AH

The Authentication Header (AH) is an IPSec protocol that provides for anti-replay and verifies that the contents of the packet have not been modified in transit.

APIC

An Advanced Programmable Interrupt Controller (APIC) is an architecture for dealing with interrupts in multi-processor computer systems.

ARP

The Address Resolution Protocol (ARP) is used to determine the Ethernet MAC address of a host when only its IP address is known.

AS

An autonomous system (AS) is a collection of IP networks and routers under the control of one entity that presents a common routing policy to the Internet.

BATV

Bounce Address Tag Validation (BATV) is the name of a method designed for determining whether the return address specified in an e-mail message is valid. It is designed to reject bounce messages to forged return addresses.

Broadcast

The address used by a computer to send a message to all other computers on the network at the same time. For example, a network with IP address 192.168.2.0 and network mask 255.255.255.0 would have a broadcast

address of 192.168.2.255.

CA

A Certificate Authority or Certification Authority (CA) is an entity or organization that issues digital certificates for use by other parties.

CBC

In cryptography, Cipher Block Chaining (CBC) refers to a mode of operation where each block of plaintext is "XORed" with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plaintext blocks up to that point.

DER

Distinguished Encoding Rules (DER) is a method for encoding a data object, such as an X.509 certificate, to be digitally signed or to have its signature verified.

DNAT

Destination Network Address Translation (DNAT) is a special case of NAT where the destination addresses of data packets are rewritten.

DNS

The Domain Name System (DNS), also referred to as *Domain Name Service*, translates the underlying IP addresses of computers connected through the Internet into more human-friendly names or aliases.

DSA

The Digital Signature Algorithm (DSA) is a standard propagated by the United States Federal Government (FIPS) for digital signatures.

DSL

Digital Subscriber Line (DSL) is a family of technologies that provide digital data transmission over the wires of a local telephone network.

ESP

Glossary

The Encapsulating Security Payload (ESP) standard is an IPSec protocol that provides data confidentiality (encryption), anti-replay, and authentication.

FTP

The File Transfer Protocol (FTP) is a protocol for exchanging files over packet-switched networks.

GRE

The Generic Routing Encapsulation (GRE) is a tunneling protocol designed for encapsulation of arbitrary kinds of network layer packets inside arbitrary kinds of network layer packets.

H.323

H.323 is a protocol providing audio-visual communication sessions on packet-switched networks.

ICMP

The Internet Control Message Protocol (ICMP) is a special kind of IP protocol used to send and receive information about the network's status and other control information.

IDENT

The Ident protocol is a standard that helps identify the user of a particular TCP connection.

IP

The Internet Protocol (IP) is a data-oriented protocol used for communicating data across a packet-switched network.

IP Address

An IP address (Internet Protocol address) is a unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP).

IRC

The Internet Relay Chat (IRC) is an open protocol enabling the instant communication over the Internet.

ISP

An Internet service provider (ISP) is a business or organization that sells to consumers access to the Internet and related services.

LSA

The link-state advertisement (LSA) is a basic communication means of the OSPF routing protocol for IP.

MAC Address

A MAC address, short for Media Access Control address, is a unique code assigned to most forms of networking hardware.

Masquerading

Masquerading is a technology based on NAT that allows an entire LAN to use one public IP address to communicate with the rest of the Internet.

MIB

A management information base (MIB) is a type of database used to manage the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.

MD5

The Message-Digest algorithm 5 (MD5) is a cryptographic hash function with a 128-bit hash value.

MIME

Multipurpose Internet Mail Extensions (MIME) is an Internet Standard that extends the format of e-mail to support text in character sets other than US-ASCII, non-text attachments, multi-part message bodies, and header information in non-ASCII character sets.

MX record

Glossary

An MX record is a type of resource record in the Domain Name System (DNS) specifying how e-mails should be routed through the Internet.

NSSA

In the OSPF protocol, a not-so-stubby area (NSSA) is a type of stub area that can import autonomous system (AS) external routes and send them to the backbone, but cannot receive AS external routes from the backbone or other areas.

NTP

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched networks.

OpenPGP

OpenPGP is a protocol combining strong public-key and symmetric cryptography to provide security services for electronic communications and data storage.

OSPF

The Open Shortest Path First (OSPF) protocol is a link-state, hierarchical interior gateway protocol (IGP) for network routing.

PEM

Privacy Enhanced Mail (PEM) is an early IETF proposal for securing e-mail using public key cryptography.

POP3

Post Office Protocol version 3 (POP3) is a protocol for delivery of e-mails across packet-switched networks.

Port

A port is a virtual data connection that can be used by programs to exchange data directly. More specifically, a port is an additional identifier—in the cases of TCP and UDP, a number between 0 and 65535 – that allows a computer to distinguish between multiple concurrent connections between the same two computers.

Protocol

A protocol is a well-defined and standardized set of rules that controls or enables the connection, communication, and data transfer between two computing endpoints.

Proxy

A proxy is a computer that offers a computer network service to allow clients to make indirect network connections to other network services.

RADIUS

RADIUS is the acronym of *Remote Authentication Dial In User Service* and is a protocol designed to allow network devices such as routers to authenticate users against a central database.

RAID

A Redundant Array of Independent Disks (RAID) refers to a data storage scheme using multiple hard drives to share or replicate data among the drives.

RBL

A Real-time Blackhole List is a means by which an Internet site may publish a list of IP addresses linked to spamming. Most mail transport agent (mail server) software can be configured to reject or flag messages which have been sent from a site listed on one or more such lists.

RED

Remote Ethernet Device. A device for branch offices and the like whose network should be secured via a remote ASG.

Router

A router is a network device that is designed to forward packets to their destination along the most efficient path.

RPS

RED Provisioning Service. An Astaro service RED devices and RED hubs register with and RED devices fetch their configuration from.

SIP

The Session Initiation Protocol (SIP) is a signalization protocol for the setup, modification and termination of sessions between two or several communication partners. The text-oriented protocol is based on HTTP and can transmit signalization data through TCP or UDP via IP networks. Thus, it is the base among others for Voice-over-IP videotelephony (VoIP) and multimedia services in real time.

S/MIME

Secure/Multipurpose Internet Mail Extensions is a standard for public key encryption and signing of e-mail encapsulated in MIME.

SMP

Denotes Symmetric Multiprocessing, the use of more than one CPU.

SMTP

The Simple Mail Transfer Protocol (SMTP) is a protocol used to send and receive e-mail across packet-switched networks.

SNAT

Source Network Address Translation (SNAT) is a special case of NAT. With SNAT, the IP address of the computer which initiated the connection is rewritten.

SOCKS

SOCKS, short for "SOCKetS", is an Internet protocol that allows client-server applications to transparently use the services of a network firewall. SOCKS, often called the Firewall Traversal Protocol, is currently at version 5 and must be implemented in the client-side program in order to function correctly.

SPF

Sender Policy Framework (SPF) is an extension to the Simple Mail Transfer Protocol (SMTP). SPF allows software to identify and reject forged addresses in the SMTP MAIL FROM (Return-Path), a typical annoyance of e-mail spam.

SPI

The Security Parameter Index (SPI) is an identification tag added to the header while using IPSec for tunneling the IP traffic.

SSH

Secure Shell (SSH) is a protocol that allows establishing a secure channel between a local and a remote computer across packet-switched networks.

SSO

Single sign-on (SSO) is a form of authentication that enables a user to authenticate once and gain access to multiple applications and systems using a single password.

Subnet Mask

The subnet mask (also called netmask) of a network, together with the network address, defines which addresses are part of the local network and which are not. Individual computers will be assigned to a network on the basis of the definition.

TCP

The Transmission Control Protocol (TCP) is a protocol of the Internet protocol suite allowing applications on networked computers to create connections to one another. The protocol guarantees reliable and in-order delivery of data from sender to receiver.

TLS

Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are cryptographic protocols that provide secure communications on the Internet.

TTL

The Time-to-live (TTL) value is an 8-bit field in the Internet Protocol (IP) header stating the maximum amount of time a packet is allowed to propagate through the network before it is discarded.

UDP

The User Datagram Protocol (UDP) is a protocol allowing applications on networked computers to send short messages sometimes known as datagrams to one another.

UPS

An uninterruptible power supply (UPS) is a device which maintains a continuous supply of electric power to connected equipment by supplying power from a separate source when utility power is not available.

URL

A Uniform Resource Locator (URL) is a string that specifies the location of a resource on the Internet.

VoIP

Voice over IP (VoIP) is the routing of voice conversations over the Internet or through any other IP-based network.

VPN

A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol such as PPTP or IPsec.

WINS

The Windows Internet Naming Service (WINS) is Microsoft's implementation of NetBIOS Name Server (NBNS) on Windows, a name server and service for NetBIOS computer names.

X.509

X.509 is a specification for digital certificates published by the ITU-T (International Telecommunications Union – Telecommunication). It specifies information and attributes required for the identification of a person or a computer system.

List of Figures

1.1	IE7 Security Settings Trusted Sites Zone	3
1.2	The Initial Login Page of WebAdmin	9
1.3	Astaro Security Gateway Login Screen	10
1.4	System Dashboard of Astaro Security Gateway	12
2.1	WebAdmin	15
2.2	Example of a WebAdmin List	18
2.3	Example of a WebAdmin Dialog Box	18
2.4	Dragging an Object From the Group Tooltip <i>Networks</i>	21
3.1	Example ASG Software V7 WebAdmin Dashboard	23
4.1	Configuring Time and Date	30
4.2	Configuring Access Control	34
4.3	Configuring User Preferences	36
4.4	MyAstaro Portal	37
4.5	Licensing Warning Message	42
4.6	Licensing Overview (Classic Licensing)	43
4.7	Installing a License	43
4.8	Up2Date Overview page	45
4.9	Up2Date Progress Bar	46
4.10	Implicit Installation of Up2Date Packages	46
4.11	User Portal of Astaro Security Gateway	53
4.12	Configuring Access to the User Portal	55
4.13	Example Warning Page and its Customizable Parts	59

4.14	HTTP Downloader Page Step 1 of 3	61
4.15	HTTP Downloader Page Step 2 of 3	61
4.16	HTTP Downloader Page Step 3 of 3	62
4.17	POP3 Blocked Message	63
4.18	Configuring SNMP Queries	64
4.19	Dashboard of Astaro Command Center	67
4.20	Configuring Central Management Using an ACC V1.9 Server	69
4.21	Configuring Central Management Using an ACC V1.4 Server	71
4.22	High-Availability Status	74
4.23	Resource Usage of the Single HA or Cluster Devices	76
4.24	Configuring a Cluster	78
5.1	Users List	84
5.2	Groups List	86
5.3	eDirectory Browser of Astaro Security Gateway	88
5.4	Configuring eDirectory User Authentication	91
5.5	Configuring Active Directory User Authentication	93
5.6	Microsoft Management Console (Administrator User Object Highlighted)	95
5.7	Configuring LDAP User Authentication	96
5.8	Configuring RADIUS User Authentication	99
5.9	Configuring TACACS+ User Authentication	101
5.10	Configuring Single Sign-On	102
6.1	Network Definition List	108
6.2	Service Definitions List	111
6.3	Time Events Definitions List	114

List of Figures

7.1	Configuring Interfaces	119
7.2	Configuring Uplink Balancing	134
7.3	Multipath Rules	136
7.4	Configuring a Bridge	138
7.5	Bridging Enabled	139
7.6	Disabling Bridging	140
7.7	Static Routes Table	141
7.8	Policy Routes Table	143
7.9	Enabling OSPF	145
7.10	OSPF Area List	148
7.11	Quality of Service Status Tab	151
7.12	Quality of Service Traffic Selectors	153
7.13	Quality of Service Bandwidth Pool	155
7.14	Example PIM-SM Configuration	157
7.15	PIM-SM Interfaces List	158
7.16	PIM-SM Rendezvous Point Routers List	159
7.17	PIM-SM Routes List	160
8.1	Configuring DynDNS	168
8.2	Configuring a DHCP Relay	172
8.3	DHCP Lease Table	174
9.1	Packet Filter Rule Table	178
9.2	Packet Filter Live Log	180
9.3	Masquerading Rule List	186
9.4	NAT Rule List	187

9.5	Configuring Intrusion Prevention	190
9.6	Attack Patterns	192
9.7	Configuring Flood Protection	193
9.8	Configuring Portscan Protection	196
9.9	Intrusion Prevention Exceptions List	197
9.10	Balancing Rule List	201
9.11	Generic Proxy Rule List	202
10.1	Global HTTP Settings	208
10.2	Configuring HTTP Proxy AntiVirus and Malware Settings	212
10.3	Configuring Active Content Removal Settings	213
10.4	Configuring the URL Filtering	214
10.5	HTTP Proxy Exceptions List	218
10.6	Advanced HTTP/S Settings Part 1	221
10.7	Advanced HTTP Settings Part 2	223
10.8	Advanced HTTP Settings Part 3	225
10.9	Proxy Profile List	231
10.10	Filter Assignments List	235
10.11	Filter Actions List	236
10.12	Configuring the FTP Proxy	239
10.13	Configuring FTP Proxy AntiVirus Settings	241
10.14	FTP Proxy Exceptions List	242
10.15	Configuring Advanced FTP Proxy Settings	243
11.1	Enabling the SMTP Proxy	246
11.2	Configuring Domains and Routing Targets	247

11.3 Configuring AntiVirus Settings of the SMTP Proxy	249
11.4 File Extension Filter on the AntiVirus Tab	250
11.5 AntiVirus Check Footer on the AntiVirus Tab	252
11.6 Configuring AntiSpam Settings of the SMTP Proxy	253
11.7 Extending Sender Blacklist on AntiSpam Tab	256
11.8 Adding Expressions to the Expression Filter on AntiSpam Tab	256
11.9 Advanced AntiSpam Features on AntiSpam Tab	258
11.10 SMTP Exceptions List	259
11.11 Configuring Relaying	261
11.12 Enabling Host/Network Blacklist	262
11.13 Enabling Content Scan for Relayed Messages	262
11.14 Configuring an SMTP Profile	266
11.15 Configuring the POP3 Proxy	271
11.16 Configuring AntiVirus Settings of the POP3 Proxy	272
11.17 Configuring AntiSpam Settings of the POP3 Proxy	274
11.18 POP3 Proxy Exceptions List	275
11.19 Configuring Advanced POP3 Proxy Settings	277
11.20 E-mail Encryption Using Two Astaro Security Gateway Units	284
11.21 Configuring E-mail Encryption	284
11.22 E-mail Encryption Options	285
11.23 Internal Users List	287
11.24 S/MIME Authorities List	289
11.25 S/MIME Certificates List	291
11.26 OpenPGP Public Keys List	292

11.27 Daily Quarantine Report of Astaro Security Gateway	293
11.28 Quarantine Report Global Settings	295
11.29 Quarantine Report Exceptions	296
11.30 Advanced Quarantine Report Options	298
11.31 Mail Manager of Astaro Security Gateway	300
11.32 Mail Manager: Overview	304
11.33 Configuration of Mail Manager	306
12.1 RED: Setup Sketch	309
12.2 RED: Site Status on the Overview Page	310
13.1 Configuring VoIP SIP Settings	316
13.2 Configuring VoIP H.323 Settings	317
14.1 Configuring IM/P2P Global Settings	320
14.2 Configuring IM/P2P Advanced Settings	320
14.3 Configuring Instant Messaging Services	322
14.4 Instant Messaging Exceptions List	323
14.5 Configuring Peer-to-Peer Services	325
14.6 Peer-to-Peer Exceptions List	327
15.1 IPSec Connections List	332
15.2 IPSec Remote Gateway List	334
15.3 IPSec Policy List	336
15.4 Configuring the Local RSA Key	340
15.5 Configuring Advanced IPSec Site-to-site VPN Settings	342
15.6 SSL VPN Connection Server Configuration	345
15.7 SSL VPN Connection Client Configuration	346

List of Figures

15.8	Configuring SSL Site-to-site VPN Settings	348
15.9	Configuring Advanced SSL Site-to-site VPN Settings	349
15.10	Site-to-site VPN Certificates List	351
15.11	Certificate Authority List	354
15.12	List of Revocation Lists (CRLs)	355
15.13	Advanced Settings	356
16.1	Remote Access Installation Files in User Portal	357
16.2	Configuring SSL Remote Access	359
16.3	Configuring SSL Remote Access Settings	361
16.4	Configuring Advanced SSL Remote Access Settings	362
16.5	Configuring PPTP Remote Access	364
16.6	Configuring iPhone Remote Access Via PPTP	366
16.7	Configuring Advanced PPTP Remote Access Settings	367
16.8	Configuring L2TP Remote Access	368
16.9	Configuring iPhone Remote Access Via L2TP Over IPSec	371
16.10	Configuring Advanced L2TP Remote Access Settings	372
16.11	Configuring IPSec Remote Access	375
16.12	IPSec Policies List	377
16.13	Configuring Advanced IPSec Remote Access Settings	381
16.14	Configuring Remote Access Via Cisco VPN Client	384
16.15	Configuring iPhone Remote Access Via Cisco VPN Client	385
16.16	Configuring Advanced Remote Access Settings	387
17.1	Configuring Local Logging Settings	390
17.2	Configuring a Remote Syslog Server	392

17.3	Configuring Remote Log File Archiving	393
17.4	View Today's Log Files	395
17.5	Selecting Archived Log Files	397
17.6	Searching Log Files	397
18.1	Enabling Anonymization of User Data	401
18.2	Histogram of the CPU Utilization	402
18.3	Histogram of the Memory/Swap Utilization	403
18.4	Histogram of the Partition Utilization	404
18.5	Histogram of the Ethernet Interfaces Utilization	405
18.6	Accounting Data Sorted for Top Services	406
18.7	Histogram of Packet Filter Violations (Monthly)	407
18.8	Histogram of Intrusion Prevention Events (Monthly)	408
18.9	Ranking of Top Domains	411
18.10	Deanonymizing Single Users	413
18.11	Histogramm of the Mail Flow	414
18.12	Ranking of Most Active E-mail Addresses	414
18.13	Deanonymizing E-mail Addresses and Domains	415
18.14	Configuration of the Daily Executive Report	416
19.1	Downloading the Administration Guide of Astaro Security Gateway	418
19.2	Checking the Availability of an Host Using Ping	419
19.3	Checking a Route Using Traceroute	420
19.4	Looking up an DNS Entry Using Dig	421

Index

- A**
- ACC 67
 - ACPI (Advanced Configuration and Power Interface) 5
 - active-active 72
 - active-passive 72
 - Active Directory 87, 93
 - bind user 94
 - ActiveX 238
 - Administration Guide 418
 - administrator
 - account 9
 - e-mail address 9, 28, 52
 - password 9, 31, 49
 - username 10
 - AH 113, 330, 373
 - AIM 322
 - aliases 131
 - antispam 25, 41, 44, 53
 - antivirus 25, 40, 44, 212, 238, 240, 250, 272
 - APIC (Advanced Programmable Interrupt Controller) 5
 - Applejuice 326
 - area (basic system settings) 6
 - Ares 326
 - ARP 118
 - ARP clash 118
 - AS 149
 - ASCII 288
 - Astaro Command Center 67
 - Astaro Partner Portal 37
 - Astaro Security Gateway
 - Appliance 1, 8
 - license key 4
 - asymmetric key cryptography 281
 - audio streams 61
- B**
- authentication 9, 265, 280
 - DKIM (DomainKeys Identified Mail) 263
 - auto-MDX 74
 - autonegotiation 137
 - autonomous system 149
 - autoscroll 180
- B**
- backups 10
 - automatic 50
 - available 49, 51, 52
 - confidentiality 49
 - creation 49
 - deletion 49, 50, 52
 - download 49, 51, 52
 - encryption 49, 51
 - file extensions 49
 - import 49
 - import V6 backup 51
 - readability 48
 - restoration 13, 48, 51, 52
 - storage 48
 - bandwidth pool 155
 - Bash 7
 - Basic System Setup form 9
 - BATV 257
 - secret 264
 - bitmask 110
 - BitTorrent 326
 - blacklist 60
 - bonding 132
 - bounce 258
 - bridging 8, 138
 - broadcasts
 - logging 185
 - bugfixes See updates 44

C

- cable modem 120
- callout reply 259
- certificate
 - X.509 83, 351
- certificate authorities 9
 - VPN Signing CA 10
 - WebAdmin CA 10, 34
- Certificate Authority 351
- Certificate Revocation List 343, 355, 382
- certificates
 - IPSec 28
 - local X.509 certificate 10, 35
 - public key 35
 - self-signed 9
 - WebAdmin certificate 9, 10, 28
 - X.509 49
- Certification Authority 281, 353
- Cisco IPSec
 - iPhone 385
- cluster 72
- command line *See* console 31
- common name 94
- company logo
 - customizing 59
- company policy 58
- company text
 - customizing 59
- confidentiality footer 263
- configuration
 - basic configuration 1, 6, 8, 10
 - final configuration 1
- configuration wizard 10
 - allowed services 11
 - antivirus settings 12
 - backup restoration 13
- configuring the internal network
 - interface 11
- configuring the uplink interface 11
- Instant Messaging settings 12

- intrusion prevention settings 11
- license installation 11
- Peer-to-Peer settings 12
- skipping the wizard 10
- SMTP/POP3 settings 12
- configuring
 - basic system settings 1, 6, 8, 10
 - gateway for WebAdmin 6
 - internal network card 6
- connection problems 8
- connections
 - concurrent 117
- connection tracking 183
- connection tracking helpers 183
- console
 - Bash 7
 - shell access *See* shell access 31
- console-based installation 1
- content blocking 24
- content filtering 24, 40, 60, 229
- content removal 213
- content type 263
- context-sensitive information 17
- corporate identity 58
- cost 149
- CPU usage 24
- CRL 343, 382
- cryptography 286

D

- Dashboard 4, 12, 16, 23, 33
 - refresh rate 23
 - system information 23
- date (basic system settings) 6, 28
- DDoS 193
- dead peer detection 341, 381
- Denial of Service 193, 196
- DHCP 120, 170, 172
 - on VLAN 52
 - relay 52
- DHCP server 11
- dig 421

- digital certificates 280
- Direct Connect 326
- Distinguished Name 94
- distinguished name 92, 95, 98, 351
- Distributed Denial of Service 193
- DKIM (DomainKeys Identified Mail)
 - 263
 - key selector 263
- DN 94
- DNAT 181, 187
- DNS 109, 165, 386
 - address record *See Also* DNS, A record 248
 - A record 248
- DNS lookup 421
- DNS zone 28
- domain component 95
- domain controller 93
- Domain Name System 165
- DoS 193, 196
- downloader pages 61
- DSCP 154
- DSCP-bits 154
- DSL PPPoA 120
- DSL PPPoE 120
- DynDNS 167, 334
- E**
- e-mail
 - In-Reply-To 252
 - e-mail encryption 280
 - default policy 286
 - internal users 287
 - e-mail notifications 57, 58
 - customizing 57, 58
 - limitting 57
 - recipients 57
 - sender address 57
 - e-mail quarantine 301
 - e-mail security
 - antispam 25, 41, 44, 53
 - attachments 53
- e-mail decryption 25
- e-mail encryption 25, 28, 41
- expression filter 53
- OpenPGP 41
- phishing protection 41
- quarantine 53, 62
- Quarantine Report 54, 56
- signature 25, 41
- S/MIME 41
- whitelisting 54
- e-mail traffic 53
- eDirectory 87, 91
- eDirectory browser 87
- Edonkey 326
- encryption
 - e-mail *See* e-mail security 25
 - encrypted communication 9
 - TLS 263
- Enterprise Toolkit 7
- envelope sender 255, 275
- ESP 113, 330, 373
- Ethernet 137
 - aliases 52
- Ethernet interface 120
- executive report 416
- expression filter 256, 275
- expression filter *See* e-mail security 53
- F**
- factory reset 32
- false positives 294
- FAT 50
- file downloads 60
- file extension 213, 237, 241, 273
- file extensions 60
 - scanning 40
- filter actions 229
- filter assignment 235
- Firefox 2
- firmware updates 17, 44, 47, 48
 - automatic download 47

firmware version 23, 45
 Flash 238
 flooding 193
 flood protection 194
 footer
 confidentiality 263
 forwarder 166
 FQDN See fully qualified domain name 28
 FTP 239, 393
 FTP proxy 25, 40, 239
 fully qualified domain name 28, 387

G

gatekeeper 317
 gateway for WebAdmin 6
 generic proxy 202, 202
 Getting Started Guide 2
 Gnutella 326
 Google Talk 322
 GRE 183
 greylisting 256

H

HA 72
 H.323 154, 316
 hard disk space
 usage 24
 Hardware Compatibility List 2
 hardware compatibility list 4
 hardware detection 6
 hardware requirements 1, 2
 HA See high-availability 51
 HCL (Hardware Compatibility List) 2
 HCL (hardware compatibility list) 4
 heartbeat 72
 HELO 256, 264
 high-availability 25, 42, 118
 autojoin 79, 80
 cluster 25, 42

failover 25
 heart-beat requests 2
 high availability 72
 automatic configuration 76
 cluster 77
 hot standby 77
 hostname 28, 35
 DNS zone 28
 fully qualified domain name 28
 hot standby 72
 HTTP 208
 HTTP proxy 208
 HTTPS 208
 HTTP/S proxy 25, 40, 52, 60
 HTTPS proxy 208
 HTTP/S proxy
 blacklist 60
 categories 60
 status messages 28, 58, 60

I

IANA 113
 ICMP 112, 142, 181
 ICQ 322
 IDENT 180, 204
 IDENT Reverse proxy 202
 IKE 336, 377
 images 61
 IMesh 326
 IM/P2P
 global settings 319
 installation
 console-based installation 1
 hardware detection 6
 kernel options 5
 keyboard layout 5
 key functions during installation 5
 monitoring installation 7
 installation log 7
 installing Astaro Security Gateway

- 1
Enterprise Toolkit 7
Open Source software 7
software 1, 4
- Instant Messaging 321
instant messaging 319
- Instant Messaging
exceptions 323
- Internet Explorer 2, 209, 233
download problems 3, 35, 49, 54, 284, 288, 299, 353, 355, 396, 396, 418, 423
- Internet Media Type see content-type 263
- intrusion prevention 24, 44, 47, 52, 189
advanced settings 199
attack patterns 191
exceptions 197
global settings 189
- IP 113
literal address 264
- IPComp 339, 380
- iPhone
Cisco IPSec connection 385
L2TP over IPSec connection 371
PPTP connection 366
- IPSec 330, 373
certificate 28
passthrough 332, 375
- IPSec connections 332
- IPSec policy 336, 377
- IPSec tunnel 333, 375
- IP Security 330, 373
- IPSec VPN 341, 380
- IPS (intrusion prevention system)
See intrusion prevention 47
- IRC 323
- J
- Jabber 322
- Java 238
- JavaScript 2, 219, 238
- K
- keep-alive
NAT traversal 332, 375
- kernel 5
ACPI (Advanced Configuration and Power Interface) 5
APIC (Advanced Programmable Interrupt Controller) 5
SMP (symmetric multiprocessing) 5
- kernel log 7
- keyboard layout 5
- key size 340
- L
- L2TP 367
L2TP over IPSec 367
iPhone 371
- LAG 133
- LDAP 87, 96
- lease 174
- license agreement 9
- licenses 40
activation keys 37
active IP addresses 43
Astaro Partner Portal 37
home user license 40
installing 38, 42
license information 41
maintenance level 42
MyAstaro Portal 40
subscriptions 40, 42
trial license 11, 40
upgrade 37
validity 40, 44
- link-state 144
- link aggregation 132
- link aggregation group 133
- link state advertisements 148
- Linux 31

load balancing 201
 localhost
 SMTP exception 260, 276
 local logging 389
 log files 395
 logging 389
 logging data
 time gaps 28
 login attempts 27
 log partition 24
 logs 28

M

MAC address 137, 173
 mail exchanger 169
 Mail Manager 299
 mail relay 260
 mail *See e-mail* 53
 malware *See Also* antivirus 25, 53
 management information base 62
 management workstation 1, 6
 Manolito 326
 mapping
 MAC/IP address 173
 masquerading 11, 186, 204
 Maximum Transmission Unit 343, 383
 MD5 146, 149, 149, 331, 374
 media
 audio streams 61
 images 61
 video streams 61
 message
 size
 limitation 264
 message digest 149
 MIB 62
 MIB II 63
 Microsoft Internet Explorer 2
 MIME 213, 237, 251
 MIME type filter 251
 modem 120

Mozilla Firefox 2
 MSCHAPv2 363
 MSN 323
 MTU 343, 383
 multicast 72
 multimedia files 213
 MUTE 326
 MX record 169, 248, 258
 MyAstaro Portal 40

N

NAS identifier 100
 NAT 180, 185
 NAT traversal 332, 374
 negotiation
 TLS 263
 NetBIOS 180
 Network Address Translation 185
 network interface card
 heart-beat capable NIC 2
 PCI ID and sequence 7
 network interface cards 117
 network interface, internal
 configuring 11
 default settings 8
 network interfaces
 bitrate 24
 status 24
 network time
 server 28
 server synchronization 28, 29
 Network Time Protocol 175
 network traffic 24
 non-delivery reports 259
 not-so-stubby area 148
 notifications 28, 57
 customizing 57, 58
 e-mail 57, 58
 limitting 57
 recipients 57
 sender address 57
 SNMP 57, 58

Novell 91
NSSA 148
NTLM 209, 233
NTP 175
NTP (network time protocol) *See* network time 28
NTP Server Pool 30

O

octet 110
online help 17, 44
 update 17
OpenPGP 25, 41, 281
 public key 292
Open Source software 7
OpenVPN 358
Operating Instructions 2
organizational unit 94
OSPF 142, 144

P

packet-length
 validating 184
packet filter 177
 live log 179
packet filtering
 dropping packets 24
 rejecting packets 24
packet filter log
 WebAdmin access traffic 34
packet filter rules 52
packet flow 8
Pando 326
parent proxy
 for updates 47
partitions
 log 24, 403
 root 24, 403
 storage 403
password complexity 104
Path Maximum Transmission Unit 343, 383

pattern updates 17, 44, 47, 48
 automatic download 47
 automatic installation 47
pattern version 23, 46
peer-to-peer 319
Peer-to-Peer
 exceptions 326
Perl Compatible Regular Expressions 256, 275
PFS 338, 379
phishing 216
phishing protection 41
ping 181, 419
PKI 355
PMTU 343, 383
policy-based routing 142
policy routes 141
POP3 270
 account settings 53
 blocked messages 62
 proxy 25, 62
 quarantine 53
 servers 54
 status messages 59
POP3 proxy 270
port forwarder 202
portscan detection 195
port trunking 132
postmaster 264
PPP 142, 143, 160
PPP modem 120
PPTP 187, 363
 iPhone 366
 remote access 52
pre-installed software 1
prefetching 275, 277, 305
priority traffic 154
privacy 280
private key 281
problems
 connection 8
product version 23

- proxies
 - FTP 25, 40
 - HTTP/S 25, 40, 52
 - parent proxy *See* parent proxy 47
 - POP3 25, 62
 - SMTP 25, 52, 62
- proxy 265
- public key 281
- public key infrastructure 281, 290, 355

- Q**
- QoS *See* Quality of Service 52
- Quality of Service 52, 151
 - bandwidth pool 155
 - status 151
 - traffic selector 153
- quarantine 275, 293
- Quarantine Report 54, 56
 - hyperlinks 56
 - releasing e-mails 56
 - status messages 59
- quarantine *See* e-mail security 53

- R**
- RADIUS 87, 98
- RAID (Redundant Array of Independent Disks) 4
 - supported controllers 4
- RAM usage 24
- RAS address 332, 375
- RBL *See* Realtime Blackhole List 254
- rDNS 256
- Realtime Blackhole List 254
- Realtime Blackhole Lists 254
- recipient verification 258
- recommended reading 1
- regular area 147
- relay 172
- remote access 52, 54
 - client software 54
 - PPTP 52
 - SSL 33
 - VPN 25
- remote access clients 386
- remote gateway 333
- remote log file archiving 393
- reporting 399
- reporting data
 - time gaps 28
- resource usage 23
- restart 82
- RFC (Request for Comments) 264
- root partition 24
- routing 8, 141
- routing protocol 144
- RR 109
- RSA authentication 339
- RSA key 339
- RSA keys
 - in backups 49

- S**
- SCP 394
- searching
 - log files 397
- security certificates *See* certificates 9
- security policy 177
- sender
 - envelope 255, 275
- server
 - backend 264
 - mail
 - upstream 265
 - mail relay 265
 - smarthost 265
 - SMTP 265
 - server load balancing 200
 - setting up Astaro Security Gateway 1

setup
 initial setup 1, 35
Share 326
shared key 264
shared secret 99
shell access 31
 disabling shell access 31
loginuser 31
password 31
root 31
shut down 82
shutdown 31
single sign-on 209, 233
SIP 154, 315
site-to-site VPN 25, 52
Skype 323
smarthost 58, 265
 authentication 58, 265
 login 265
 plain 265
SMB 394
S/MIME 25, 41, 281
 authorities 289
 automatic extraction 286
 certificate 291
SMP (symmetric multiprocessing)
 5
SMTP 41, 58
 banner 264
 HELO 264
 hostname 264
 log 53
 profiles 41
 proxy 25, 52, 62, 264
 server 265
 TLS 58
SMTP profile 265
SMTP proxy 245
SNAT 181, 187
SNMP 57, 58
 community string 64
 queries 64
traps 65
SOCKS 4 203
SOCKS 5 203
SOCKS proxy 202
software
 preinstalled software 1
software installation 1, 4
spam 253, 254, 273
 RBL See Realtime Blackhole Lists
 254
 reduction 254
spam marker 255, 275
spam protection 25, 41, 44, 53
spam purveyors 25
spam releasing
 mailing list 294
SPF 257
SPI 113
split tunneling 359
spoof protection 184
spyware 208, 215, 237
spyware protection 25, 40, 60
SSH (secure shell) 31
 client 31
 daemon listen port 31
SSL 358
SSL remote access 33
SSL VPN 358
static MAC/IP mapping 173
static routes 141
strict policy 339, 380
strict routing 333
strict TCP session handling 184
stub area 147
subnetwork 110
subscriptions 42
 Mail Encryption 41
 Mail Filtering 41
 warning message 41
 Web Filtering 40
support 13
 contact 418

ticket 418
 swap usage 24
 switch
 jumbo frame support 2
 SYN (TCP) flood protection 194
 Syslog 391
 system configuration 24
 system messages 58
 templates 62
 Unicode 58
 UTF-8 58
 system requirements 1, 2
 for WebAdmin access 2
 system settings, basic
 administrator account 9
 area 6
 Basic System Setup form 9
 company information 9, 28
 configuration of 1, 6, 8, 10
 date 6, 28
 hostname 28, 35
 internal network card 6
 license agreement 9
 time 6, 28, 29, 35
 time zone 6, 28, 35
 wizard See *Also* configuration wizard 10

T

TACACS 87, 100
 TCP 111, 112
 TCP/IP stack 184
 TCP window scaling 184
 Tencent QQ 323
 three-way handshake 184
 time (basic system settings) 6, 28, 29, 35
 time event 114, 179, 235
 time zone (basic system settings) 6, 28, 35
 TLS 58
 TOS 154
 TOS-bits 154
 totally stubby area 148
 traceroute 182, 420
 traffic See network traffic 24
 traffic selector 153
 traffic shaping 151, 152
 transparent mode 210, 221, 233, 277
 TTL 109
 Type of Service 154, 343, 382

U

UDP 111, 112
 uninterruptible power supply 2, 3
 APC 4
 automatic recognition of 4
 battery mode 4
 MGE UPS Systems 4
 notifications 4
 status 24
 supported manufacturers 4
 unit
 base-2 407, 410
 units of measurement 404
 updates 44
 automatic download 47
 available 23, 45
 firmware updates See firmware updates 44
 installing 45
 manual updates 48
 parent proxy 47
 Up2Date packages 44
 update servers 44
 UPS *see also* uninterruptible power supply 3
 UPS (uninterruptible power supply) 2
 status 24
 uptime 23
 USB device
 restoring backup from 50

- user
 - creating automatically 89
 - user authentication
 - remote 52
 - user groups 52
 - user messages *See* system messages 62
 - User Portal 33, 53, 301
 - access 53, 54
 - allowed networks 55
 - allowed users 55
 - hostname 55
 - language 55
 - login 56
 - logout 54
 - port 55
 - SMTP log 53
 - SMTP quarantine 53, 62
 - welcome message 56
 - user profiles
 - language setting 32
 - utilization
 - interfaces 404
 - V**
 - video streams 61
 - virus protection 25, 40, 44
 - virus scanner 59, 60
 - virus scanning 208
 - e-mails (SMTP) 249, 272
 - FTP traffic 240
 - web traffic 211
 - VLAN 120
 - VoIP 154, 316
 - VPN 187
 - remote access 25, 52
 - site-to-end 357
 - site-to-site 25, 52, 329
 - VPN tunnel 333
 - W**
 - web-based administrative interface
- ASG V7 Administration Guide*
- See WebAdmin 1
 - WebAdmin 1, 8, 15, 27
 - access traffic, monitoring 34
 - administrator access 33
 - auditor access 33
 - button bar 17
 - certificate 9, 10, 28
 - certificate authority 10, 34
 - dialog box 18
 - drag-and-drop functionality 18
 - idle timeout 17, 33
 - info icon 18
 - language 32
 - login 10, 35
 - logout 17
 - logout, automatic 17, 33
 - menu structure 15
 - networks, allowed 33
 - online help 17
 - page reload 17
 - password guessing, blocking 34
 - security warnings 35
 - TCP port 32
 - web browser and proxy 3
 - web browser compatibility 2
 - web filtering *See Also* content filtering 25
 - web of trust 282
 - website categories 216
 - Windows 93
 - WinMX 326
 - Winny 326
 - WINS 171, 386
 - workstation
 - management 1, 6
 - worms *See Also* antivirus 25

X

 - X.500 96, 281
 - X.509 351
 - X.509 authentication 341, 380
 - X.509 certificate 83

X.509 certificates
 in backups 49
Y
Yahoo! Messenger 323

Z
ZIP
 encrypted 213, 241, 252, 273