Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0356-2006

for

Astaro Security Gateway (ASG)
Version 6.300

from

Astaro AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5455, Infoline +49 (0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0356-2006

Astaro Security Gateway (ASG) Version 6.300

from

Astaro AG

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.3* (ISO/IEC 15408:2005) or conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

PP Conformance:	**Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999**
Functionality:	**PP conformant (plus product specific extensions)** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL2 augmented by ALC_FLR.1 – Basic flaw remediation**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, September 25th, 2006

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-5455 - Infoline +49 228 9582-111

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Astaro Security Gateway (ASG), Version 6.300 has undergone the certification procedure at BSI.

The evaluation of the product Astaro Security Gateway (ASG), Version 6.300 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The vendor and developer is:

Astaro AG
Amalienbadstraße 36
76227 Karlsruhe, Germany

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on September 25th, 2006.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-18.

The product Astaro Security Gateway (ASG), Version 6.300 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Astaro AG
Amalienbadstraße 36
76227 Karlsruhe, Germany

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The TOE Astaro Security Gateway (ASG), Version 6.300 is a packet filtering firewall based on a Linux Operating System environment.

The Astaro Security Gateway resides between the network which it is protecting and an external network such as the Internet. It can be used in a wide range of network environments from the small and home office to large enterprises.

A separate management console called WebAdmin is the web-based GUI administering Astaro Security Gateway.

The Astaro Security Gateway is either available as ASG Software (delivered as a CD package or by download from the Astaro website), or as a hardware unit called ASG Appliance, having ASG Software preinstalled. For more information about the packages being part of the TOE and the appliances itself please refer to chapter 2 of this report.

The IT product Astaro Security Gateway (ASG), Version 6.300 was evaluated by atsec information security GmbH. The evaluation was completed on September 11th, 2006. The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The vendor and developer is

Astaro AG
Amalienbadstraße 36
76227 Karlsruhe, Germany

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL2 (Evaluation Assurance Level augmented by ALC_FLR.1 – Basic flaw remediation).

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 conformant as shown in the following tables.

[8] Information Technology Security Evaluation Facility

The following SFRs are taken from CC part 2:

Security Functional Requirement	Addressed issue
FAU	**Security Audit**
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FDP	**User data protection**
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_RIP.1	Subset residual information protection
FIA	**Identification and authentication**
FIA_ATD.1	User attribute definition
FIA_SOS.1	Specification of secrets
FIA_UAU.1	Timing of authentication
FIA_UID.2	User identification before any action
FMT	**Security Management**
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security Roles
FPT	**Protection of the TOE Security Functions**
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation

Table 1: SFRs for the TOE taken from CC Part 2

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.1.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
FDP	**User data protection**
FDP_RIP.1	Subset residual information protection
FPT	**Protection of the TOE Security Functions**
FPT_SEP.1	TSF domain separation
FPT_RVM.1	Non-bypassability of the TSP
FPT_STM.1	Reliable time stamps

Table 2: SFRs for the IT-Environment

Note: Only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.3.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
F.HMI	The TOE provides the administrator with the capability to 5 perform Human-Machine-Interface (HMI) functions in order to administer the TOE and review the audit records.
F.AUDEVT	Generation of audit records.
F.AUDINF	Necessary information a audit record has to contain
F.AUDRPT	Authorized access to the audit records
F.AUDSTO	Protection of audit records
F.FWRULES	Use of a security policy to restrict the ability of unauthenticated external IT entities to pass information to one another through the TOE.
F.FWINVOKED	The TOE ensures that all information flows provided to the TOE by external entities for transfer to other entities are subjected to the defined security policies and conform to them before they are allowed to proceed toward the destination entity.
F.ADMIN	Access to the TOE is restricted to administrators only. Each administrator has a set of privileges consistent with F.HMI which only allow the administrators to perform those tasks associated with their duties.
F.I&A	Authentication based on passwords and a password policy.
F.NORESID	The TOE ensures that no information from previously processed information flows is transferred to subsequent information flows.

TOE Security Function	Addressed issue
F.INIT	The TOE provides restrictive default values for information flow security attributes that are used to enforce the SFP, and allows the administrator to override the default values when an object or information is created.

Table 3: Security Functions of the TOE

Only a short summary of the Security Functions has been provided in the table above. For more details please refer to the Security Target [6], chapter 6.2.

1.3 Strength of Function

The TOE's strength of functions is claimed 'basic' (SOF-basic) for specific functions as indicated in the Security Target chapter 5.1.1.2 and 8.5. It is claimed for the Security Function F.I&A which is concerned with the password based authentication.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The threats discussed below are all taken from the Protection Profile the TOE claims conformance to. The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself. The threat agent is assumed to be an independent attacker with a low level of sophistication who is attacking simply for the thrill of doing so, without a specific agenda. The resources are assumed to include only those attack tools that are publicly available.

T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.REPEAT An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

T.REPLAY An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.

T.ASPOOF An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.

T.MEDIAT An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.

T.OLDINF Because of a flaw in the TOE's functioning, an unauthorized person may gather residual information from a previous

information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

T.PROCOM An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

T.AUDACC Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data.

T.AUDFUL An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.

Please note that no Organizational Security Policies (OSPs) have been claimed in the Security Target.

1.5 Special configuration requirements

The TOE software runs on top of a Linux operating system, which is delivered with the ASG product, but considered to be part of the TOE environment. Certain Linux modules have been altered to provide specialized functionality for ASG. In addition, the TOE also comprises security enforcing packages created by Astaro. For a detailed listing of the TOE packages please refer to chapter 2 of this report.

The Linux OS is automatically hardened and configured by the installation scripts of the ASG software. Whereas the configuration scripts and their effect are part of the TOE, the services and files configured are, with the exceptions of the TOE packages as listed in chaper 2 of this report, part of the TOE environment.

1.6 Assumptions about the operating environment

The operational environment has to meet the following assumptions. They are given by the Protection Profile the TOE claims conformance to.

In general the PP assumes that conformant TOEs are intended to be used either in environments in which, at most, sensitive but unclassified information is processed or the sensitivity level of information in both the internal and external networks is equivalent. Although language of the PP is aimed at government environments the TOE is also intended to be used in commercial environments.

A.PHYSEC The TOE is physically secure.

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.PUBLIC The TOE does not host public data.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

A.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

A.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

In addition to the assumptions of the PP the following is assumed for the operational environemtn by the ST:

A.CONSOLE A securely-configured management console, in the same physically-secure location as the TOE, is directly connected to the TOE via a dedicated link entirely within a controlled area of the environment. The console is expected to correctly transmit the information entered on it to the TOE; and to correctly display the information sent to it by the TOE.

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Astaro Security Gateway (ASG), Version 6.300

The TOE is software and runs on top of a Linux operating system, which is delivered with the ASG product, but considered to be part of the TOE environment. Certain Linux modules have been altered to provide specialized

functionality for the TOE. In addition, the TOE also comprises security enforcing packages created by Astaro. The follwing packages are relevant in that respect:

- iptables-1.3.1-13.i686.rpm
- netfilter-tools-6.1-11.i686.rpm
- syslog-ng-1.6.7-7.i686.rpm
- ulogd-1.23-9.i686.rpm
- ep-aua-6.2-67.i686.rpm
- ep-webadmin-6.3-88.i686.rpm

The Linux OS the TOE is running on is automatically hardened and configured by the installation scripts of the ASG software. Whereas the configuration scripts and their effect are part of the TOE, the services and files configured are, with the above exceptions, part of the TOE environment.

The Astaro Security Gateway is either available as ASG Software (delivered as a CD package or by download from the Astaro website), or as a hardware unit called ASG Appliance, having ASG Software preinstalled.

The following models of ASG Appliances running the ASG Software exist: ASG110, ASG120, ASG220, ASG320, ASG425, ASG525, ASG525F. For more details on the appliances and the Interfaces they offer, please refer to the ST chapter 1.2.

If the TOE is downloaded via the Astaro website the customer has to ensure the authenticity and integrity of the download package by verifing a cryptograpghic checksum. This procedure is described as part of the CC Guidance Documentation [1] also beeing part of the TOE (for more information about guidance documents please refer to chapter 6 of this report).

3 Security Policy

The TOE implements a single information flow control Security Function Policy (SFP). The information flow control SFP is called the UNAUTHENTICATED SFP. The subjects under control of this policy are external IT entities on an internal or external network sending information through the TOE to other external IT entities. The information flowing between subjects in the policy is traffic with attributes, defined in the SFR element FDP_IFF.1.2, including source and destination addresses. The rules that define each information flow control SFP are found in FDP_IFF.1.2. The security functional requirement FMT_MSA.3 demands that these rules be assigned restrictive initial values. FMT_MSA.1 ensures that the rules are subsequently managed only by the authorized administrator.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Please refer to chapter 1.6 for a complete listing of the assumptions which has to be met by the TOE environment. All assumptions except A.CONSOLE are defined by the Protection Profile the TOE is claiming conformance to.

4.2 Environmental assumptions

Please refer to chapter 1.6 for a complete listing of the assumptions which has to be met by the TOE environment. All assumptions except A.CONSOLE are defined by the Protection Profile the TOE is claiming conformance to.

4.3 Clarification of scope

The following threat has to be countered by the TOE environment:

T.TUSAGE The TOE may be inadvertently delivered, configured, used and administered in an insecure manner by either authorized or unauthorized persons.

5 Architectural Information

General Overview:

ASG Software is a network security application which includes a firewall in order to control network access. The firewall is used for perimeter security in which it controls the data transferred between two networks of which one is called to be “external” and the other one which is called “internal”. The internal network and its assets are also protected by the firewall from unauthorized access. ASG Software is also capable of controlling the data stream between multiple networks or segments.

The following figure shows a typical scenario in which ASG Software is deployed between an external and internal network.

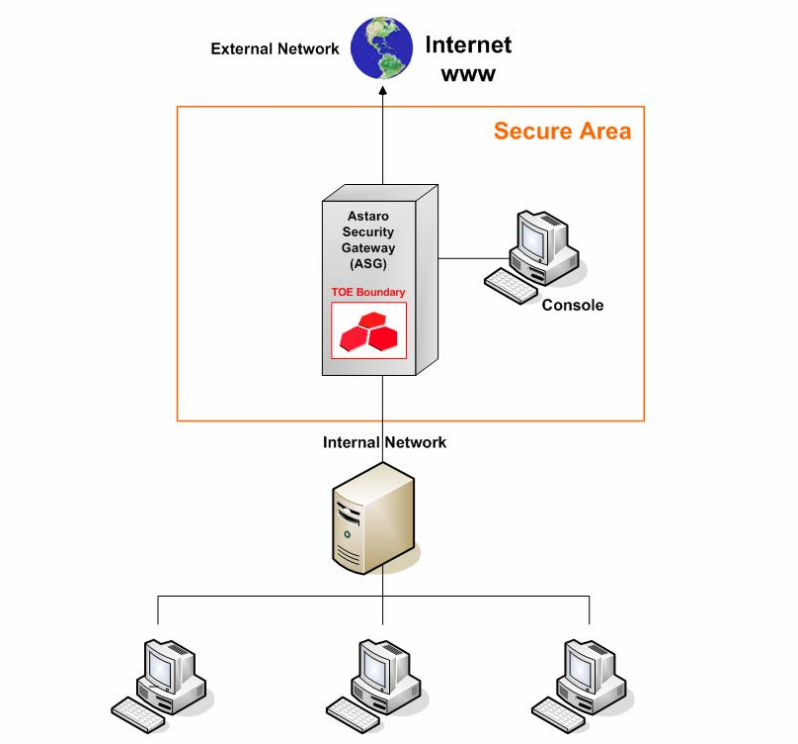

Figure 1: Typical ASG Network Configruation

The Target of Evaluation (TOE) consists of the ASG Software firewall components which manage data traffic between networks according to configurable rule-based procedures (the Packet Filter).

The Packet Filter allows for selective passing or blocking of data packets as they pass through network interfaces.

The following picture shows the overall ASG architecture and the relation of TOE to non-TOE components. The TOE that has been subject to the evaluation encompasses the core firewall functionality and its management components:

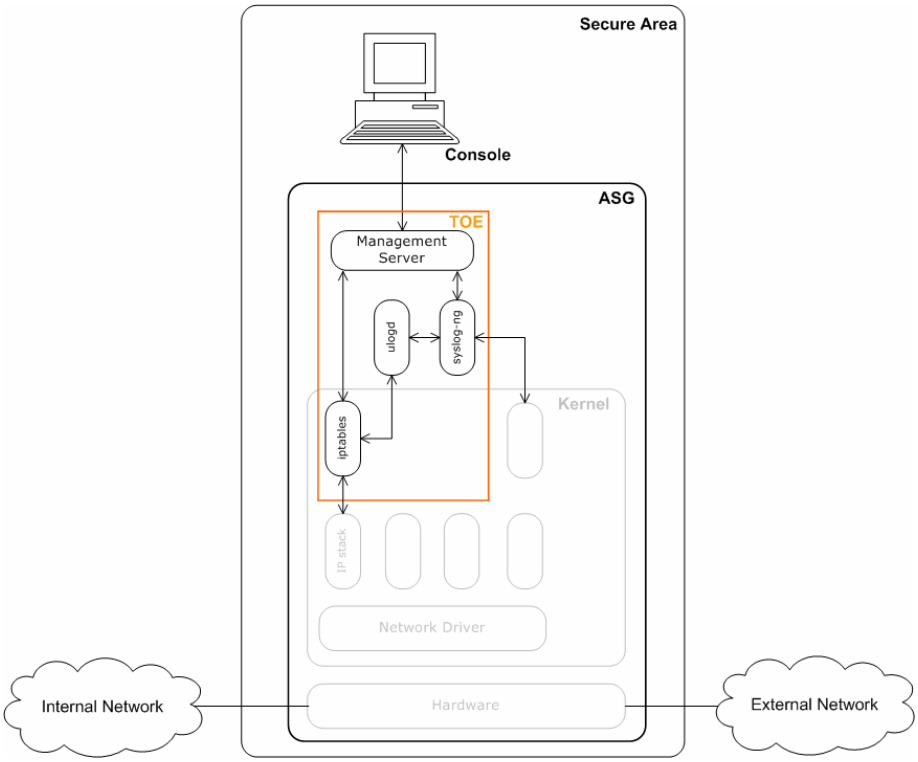

Figure 2: ASG Architecture

ASG Software is designed to be installed and used in an environment which is configured and controlled in accordance with the administrator's and CC guide ([10] and [9]) that is shipped together with the software.

ASG software is administered from a console directly connected to the firewall within the secure area. No remote administration is anticipated.

TOE Boundary and Runtime Environment:

The figure above presents an abstract overview of the TOE, its general IT environment, and identifies the TOE boundary. The following will give a more detailed overview of the technology that has been used to build the TOE and the underlying system that is expected to provide the runtime environment for the TOE.

The Management Server consists of a set of web pages and CGI scripts that provide the GUI to the administrator working at the locally attached console, and translate the administrator's actions initiated at this GUI into the appropriate commands and configuration file updates in the ASG. Administrator actions may affect the TOE itself (e.g. when changing firewall rules or viewing audit logs), or the runtime environment (e.g. when setting the system's clock). The HTTP service itself is provided by an underlying web server, which is not part of the TOE, but belongs to the TOE environment.

The packet filtering functionality of ASG is provided by the iptables module of the kernel. Based on the standard iptables component of the Linux Kernel, Astaro has modified this component to provide a more robustness and better

performance. In addition to the kernel module, this component also provides the iptables userspace command necessary to configure all aspects of the kernel module. Iptables is considered a (logical) interface to the TOE through which the IP packets arrive at the TOE.

Additionally two logging components are part of the TOE: ulogd is the userspace logging daemon for all netfilter/iptables related logging. It is part of the netfilter/iptables framework. The standard syslog-ng is required for all logging and has been added to the TOE because it has not yet been part of an evaluation of Linux.

For the underlying operating system, which is part of the TOE environment, ASG uses a standard Linux kernel. ASG is based on the SuSE Linux Enterprise Server version 9 (SLES9) distribution, which has already been successfully evaluated at the Common Criteria assurance level EAL4. The main differences between the already evaluated components and the components distributed by ASG are as follows:

- ASG only includes the components absolutely necessary to support the ASG functions
- During installation, the components are automatically configured in a secure manner.
- Some components not relevant to security have been modified to tailor the system to its special purpose as a security gateway rather than a generalpurpose computing system, and to enhance its performance.

TOE Security Functionality

The TOE provides the following security functionality:

- Access Control
  The TOE provides a role based access control capability that ensures that only authorized administrators are able to access and administer the TOE.
- Information Flow Control
  The information flow is restricted by default but permitted by set of rules that have to be defined by an authorized administrator, thus implementing stateful inspection.
- Logging
  The TOE performs logging and data is either stored in memory or written to a hard disk. Events that are recorded consist of the following:
  - Administrative events, such as system configuration changes
  - Network anomalies, which may be associated with attacks
  - Traffic events, associated with session establishment and packet information flow
- Administration
  On all gateways a direct x-over Ethernet cable can be connected to an

Ethernet port that has been configured for administrative use. When connected to an appropriate computer this port provides direct local access to the GUI and allows an authorized administrator to configure ASG Software, monitor its operation, examine the audit logs that are created, and perform backup and archive activities.
Administration handling is provided by a separate user authentication daemon called AUA which operating system independently processes all authentication requests.

6 Documentation

To install and configure the TOE such that it matches the configuration described in the Security Target the user has to follow the guidance provided in [10] and [9]:

- The CC-guide [9] represents an additional document especially written to install, configure and operate the TOE in the CC compliant mode. If functions are described in [10] and [9] the instructions in the [9] have to be followed first.
- The Web-Administration Guide [10] is the general guidance document for administrators to install, configure and operate the Firewall developed by Astaro AG.

7 IT Product Testing

The test platform was set up by the developer according to the ST and all relevant guidance, ensuring that the evaluated configuration as defined in the ST was tested. This among other things means that the software only version of the TOE and the TOE running on the appliances as listed in the ST have been tested during the evaluation.

The developer test scrips were performed successfully on the evaluated configuration of the TOE. Test coverage as required by the CC for EAL 2 was achieved. The overall test depth of the developer tests comprises the functional specification also as required for the assurance level of the evaluation.

A selected subset from the developer tests have been successfully repeated by the evaluation facility. In some areas the test coverage of the developer was supplemented by independent evaluator testing. The achieved test results matched the expected results as documented by the developer in the developer test documentation.

Furthermore, a set of independent penetration tests has been performed by the evaluation facility without being able to successfully penetrating the TOE.

8 Evaluated Configuration

The Target of Evaluation Astaro Security Gateway (ASG), Version 6.300 runs on top of a Linux operating system, which is delivered with the ASG product, but

considered to be part of the TOE environment. Certain Linux modules have been altered to provide specialized functionality for the TOE. More details about those modules can be found in chapter 2 of this report or in chapter 2.3 of the ST.

The Astaro Security Gateway is either available as ASG Software (delivered as a CD package or by download from the Astaro website), or as a hardware unit called ASG Appliance, having ASG Software preinstalled. More details about the appliances and the steps required for the downloading of the software are provided in chapter 2 of this report.

The guidance documentation [9] and [10] have to be followed to securely install and configure the TOE.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL2.

All CC, Part 3 assurance components according to EAL2 (refer to [1], part 3, chapter 11) augmented by ALC_FLR.1 – Basic flaw remediation and the class ASE for the Security Target evaluation) have been assessed with a PASS verdict.

The evaluation has shown that:

- the TOE is conformant to the PP [8]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL2 augmented by ALC_FLR.1 – Basic flaw remediation.
- The following TOE Security Functions fulfil the claimed Strength of Function: SF F.I&A (Authentication based on Passwords): SOF-basic

The results of the evaluation are only applicable to the TOE as specified by chapter 2 of this report in the configuration as detailed by the ST and the user guidance documents as listed in chapter 6 of this report.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The guidance documents [9] and [10] as well as the Security Target [6] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-CC-0356, Version 2.08, September 4th, 2006, Security Target for Astaro Security Gateway Software V6.300 CC Compliant Software, Astaro AG

[7] Evaluation Technical Report BSI-DSZ-CC-0356, 2.0, September 10th, 2006, atsec information security GmbH (confidential document)

[8] U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999

[9] CC-Guide for Astaro Security Gateway V6.3, File: CC_Guide.pdf

[10] Astaro Security Gateway V6.300 WebAdmin User Manual, File: ASG-V6-300-SW-UserManual-EN.pdf, Version: 3.00

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

a) **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

b) **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

a) **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Assurance categorisation (chapter 7.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”