Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0696-2011

for

Astaro Security Gateway V8 Packet Filter Version 1.000, secunet wall 2 packet filter Version 1.000

from

Astaro GmbH & Co. KG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0696-2011

Packet Filter

Astaro Security Gateway V8 Packet Filter Version 1.000, secunet wall 2 packet filter Version 1.000

from	Astaro GmbH & Co. KG
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2

Common Criteria
Recognition
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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.

Bonn, 3 June 2011

For the Federal Office for Information Security

SOGIS
IT SECURITY CERTIFIED

Bernd Kowalski
Head of Department

L.S.

This page is intentionally left blank.

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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification.....7

1 Specifications of the Certification Procedure.....7

2 Recognition Agreements.....7

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA).....7

2.2 International Recognition of CC – Certificates (CCRA).....8

3 Performance of Evaluation and Certification.....8

4 Validity of the Certification Result.....9

5 Publication.....9

B Certification Results.....11

1 Executive Summary.....12

2 Identification of the TOE.....13

3 Security Policy.....14

4 Assumptions and Clarification of Scope.....15

5 Architectural Information.....15

6 Documentation.....16

7 IT Product Testing.....16

7.1 Developer Testing.....16

7.2 Evaluator Independent Testing.....17

7.3 Evaluator Penetration Testing.....17

8 Evaluated Configuration.....19

9 Results of the Evaluation.....19

9.1 CC specific results.....19

9.2 Results of cryptographic assessment.....19

10 Obligations and Notes for the Usage of the TOE.....19

11 Security Target.....20

12 Definitions.....20

12.1 Acronyms.....20

12.2 Glossary.....21

13 Bibliography.....22

C Excerpts from the Criteria.....23

D Annexes.....33

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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 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 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

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 V8 Packet Filter Version 1.000, secunet wall 2 packet filter Version 1.000 has undergone the certification procedure at BSI.

The evaluation of the product Astaro Security Gateway V8 Packet Filter Version 1.000, secunet wall 2 packet filter Version 1.000 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 24 May 2011. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Astaro GmbH & Co. KG.

The product was developed by: Astaro GmbH & Co. KG.

[6] Information Technology Security Evaluation Facility

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. 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 and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Astaro Security Gateway V8 Packet Filter Version 1.000, secunet wall 2 packet filter Version 1.000 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Astaro GmbH & Co. KG
An der RaumFabrik 33a
76227 Karlsruhe

This page is intentionally left blank.

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.

1 Executive Summary

The Target of Evaluation (TOE) is the product Astaro Security Gateway V8 Packet Filter provided by Astaro GmbH & Co. KG. The TOE is a packet filter and allows the integration of packet filtering capability into a firewall or VPN components which are parts of the Astaro Security Gateway product family. The packet filter has to be delivered to an application developer.

The application developer integrates the Astaro Security Gateway V8 Packet Filter into an application in order to build a network component. The administrator of this application is defined as the TOE end-user. The evaluation of the TOE also includes its OEM version “secunet wall 2 packet filter”. This OEM version of the TOE is technically identical with the TOE, but only differs in terms of the name. The OEM version of the TOE has exactly the same security functions as the TOE itself.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] chapter 5.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionalities:

TOE Security Functionality	Addressed issue
Information Flow Protection	The TOE enforces the Packet Filter information flow policy. This policy ensures that the TOE will only forward data from and to the internal network if the information flow policy allows it. Therefore the TOE implements the information flow control (as routers) on the network layer (IP) and transport layer (TCP/UDP/ICMP).
Security Audit	The TOE collects audit data and sends it to a memory buffer in order to identify attempts to violate a policy. This allows the authorized administrator to inspect the current state of a network component.
Management	The TSF is capable of performing the following management functions: • Modification of network traffic filter rules • Modification of configuration data The TOE verifies the identification information of an administrator provided by the environment (application) before any management function can be performed. The TOE is initialized with a strict packet filter rule set, that is, everything is dropped.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 6.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapters 3.4, 3.5 and 3.6.

For the configuration of the TOE covered by this certification please refer to chapter 8 of this report.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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 V8 Packet Filter Version 1.000, secunet wall 2 packet filter Version 1.000

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW (source code)	Astaro Security Gateway V8 Packet Filter	ASGPF-1.000-4	Physically via CD-ROM
2	DOC	Manual for application developers [9]	0.95	
3	DOC	Flaw remediation [10]	0.93	
4	DATA	Release Notes	1.000-4	
5	DATA	Public verification key	N/A	
6	DATA	Signed checksum file	N/A	
7	SW (binary)	Astaro Security Gateway V8 Packet Filter: • Linux kernel with TOE parts • Module configuration IPv4 • Module configuration IPv6 • Module log IPv4 • Module log IPv6 • Module filter IPv4 • Module filter IPv6 • Module IPv6 Kernel Stack	ASGPF-1.000-4	

Table 2: Deliverables of the TOE

The software consists of eight binary files which can be uniquely identified by their hash checksums. The following table lists, where applicable, the SHA-256 checksums of all TOE components.

No	Identifier	SHA-256 checksum
1	Astaro Security Gateway V8 Packet Filter	-
2	Manual for application developers	e7a28ac6da23d940af2eca66209cdaf5b41cec9136893e18389f2737b22d4e67
3	Flaw remediation	8d44a0e6ada6582a95d379288dbc3a7e4f1f77179f2444a5d12cca2b873312f0
4	Release Notes	cf1807c1a73ab6cac852533926b3ddb95dded5efb4df02dbc43e2cb2cb5d23ef
5	Public verification key	77dfa7991d784e93758661874bd8994fd19a9183df6a91048f3ca4347b3c460f
6	Signed checksum file (sha256sums.asc)	-
7.1	Linux kernel with TOE parts	55078b6dc15180c18688b7849578f49689e865ec353f241f2bf5930e44e5dd73
7.2	Module configuration IPv4	cc9b353552cb21e0cde1b82e2e8b6f51c254f1f201a5e9686afad53f2ca3dd52
7.3	Module configuration IPv6	35c00d6e10ed54eaac46e036105fa685756d7f831943db18d89756bd6cb3e399
7.4	Module log IPv4	a671567fe16446be79961b768c467732d8ec70285c75c7cc7a5d541e13851bcf
7.5	Module log IPv6	303f90c7f07a561724264952e6dc4d3307e2c5879f3f4fb498c456a003abf669
7.6	Module filter IPv4	edf473f4d40285c0529fc5f87b9460d43a502b7c85ce9c5ee8afe366d03e9d4e
7.7	Module filter IPv6	c6bcce135707cb042598960e33940bff1ada444df9efca49ca31f488b6e0452a
7.8	Module IPv6 Kernel Stack	5d8e076bb8c5c20c051e315ed0a7326956301a316619a2617212a0cc16a6d546

Table 3: SHA-256 Checksums

The TOE is personally delivered on a CD to the application developer. The project manager describes the integrity and authentication checks to the application developer. The application developer and the end-user can verify that the authenticity and integrity of the TOE has not been altered. First the signed checksum file must be verified. Therefore the user uses the public verification RSA key with the SHA-256 fingerprint described above. After a successful verification of the checksum file the hash values of the binary parts of the TOE stated in this file can be compared to the calculated ones. This calculation can be done with any available SHA-256 program.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Information Flow Protection: The TOE enforces the Packet Filter information flow policy.
- Security Audit: The TOE collects audit data and sends it to a memory buffer in order to identify attempts to violate a policy.

- Management: The TSF is capable of performing the following management functions:
  - Modification of network traffic filter rules
  - Modification of configuration data

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- The TOE is used in a controlled environment. Specifically it is assumed:
  - That only the administrator gains physical access to the TOE,
  - That the administrator handles the authentication secrets with care, specifically that he will keep them secret and can use it in a way that nobody else can read it.
- The administrator of the TOE is non hostile, well trained and knows the existing documentation of the TOE. The administrator is responsible for the secure operation of the TOE.
- The TOE is securely initialised, i.e. that the initialisation is done according the procedure described in the documentation.
- No information can flow between the internal and external networks unless it passes through the TOE.
- The network components (TOE and application) are configured in a secure manner. Specifically it is assumed that no incoming connections are accepted except protected data (e. g. SSH) from the management machine.
- The data flow between the management machine and the network components is protected by cryptographic transforms (e. g. SSH authorization and SSH transport protection).
- The IT environment provides a Syslog server and a means to present a readable view of the audit data.
- The environment allows the Identification and Authentication of an administrator.

Details can be found in the Security Target [6], chapter 3.4.

5 Architectural Information

The TOE is a packet filter. The Astaro Security Gateway V8 Packet Filter consists of software on machines to implement packet filter functionality for the network components; i.e. the Astaro Security Gateway V8 Packet Filter is part of the network components. The packet filter relies on information available at OSI layer 3 and layer 4 for policy enforcement. The functionality for packet filtering is part of the operating system (Linux). The Astaro Security Gateway V8 Packet Filter supports IPv4 and IPv6 protocol.

The security functions of the TOE are:

- SF.1 Information Flow Control
- SF.2 Security Audit

- SF.3 Management

These security functions are enforced by the following subsystems:

- IPv4 Kernel Stack (supports the TSF SF.1)
- IPv6 Kernel Stack (supports the TSF SF.1)
- Netfilter (supports the TSFs SF.1, SF.2 and SF.3)
- “/proc file system” (supports the TSF SF.3)
- User-Space I/O (supports the TSF SF.3)

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

7.1 Developer Testing

TOE Test Configuration

The TOE was tested on a stand-alone computer with three virtual workstations. The TOE was running in a virtual machine which was configured according to chapter 1.2.2 of [6].

Besides the requirements described in chapter 1.2.2 of [6] the test environment also needed to fulfil the security objectives for the environment. These security objectives were fulfilled by the services which were installed on the virtual machine. The needed components are described in the application developer guidance [9]. The TOE environment and the related test equipment for the tests were consistent with the ones described in [6] and in the application developer guidance.

The tests of the TOE were carried out by executing the test environment. The virtual workstations provided two standard workstations and one with the TOE installed. The used non-TOE hardware for the test environment were a computer with an Intel x86-64 compatible CPU, a PCI bus system, 512 MB RAM, three 100Mbit/1000Mbit networking cards, a hard drive and a CD drive.

Testing Approach

The developer specified and implemented test cases for each defined subsystem. The test cases divided into those of the IP Kernel Stack, the Netfilter, the User-Space I/O and Netfilter and the User-Space I/O and /proc file system. Thus all subsystems are covered by several test cases and each SFR-enforcing module is covered by at least one test case.

For the tests of the TOE the developer used the test environment with three virtual workstations. This test environment consists of an executable bash script that starts up the virtual machines and initializes the complete test network. Then each test case is located in one bash script. If a test case script is executed the packets are generated and the evidence is written into log files. The developer carried out interactive as well as non-interactive tests. Altogether there are 74 test cases with more than 930 single tests covered by the test specification.

Conclusion

The results of the TOE tests prove the correct implementation. All test cases were executed successfully and ended up with the expected result.

7.2 Evaluator Independent Testing

TOE Test Configuration

The TOE can have only one configuration. The TOE separates two networks from another (see chapter 1.2.1 of [6]). For testing the TOE the evaluators used three virtual workstations. Two of these virtual machines simulate the different networks and on the third machine the TOE is installed. The virtual host is able to start tests and is used as a management workstation.

The following configuration

> PC with Intel Pentium IV compatible 2.69 GHz, 128 MB RAM, GNU/Linux 2.6.32 and installed Astaro Security Gateway V8 Packet Filter, secunet wall 2 packet filter with three external Ethernet interfaces

is the configuration of the virtual machine and is consistent with the one described in [6]. The evaluator also has started the TOE without a virtual environment. This installed TOE showed the same properties as the TOE in the virtualized environment.

Testing Approach

The evaluators repeated all developer tests in the evaluator's lab. The reason why the evaluators repeated all developer tests is that all tests are important for a correct implementation of the security relevant functionality of the TOE.

The newly added independent evaluator tests were done to verify the security provided by the TOE. Therefore TCP and UDP packets using IPv4 and IPv6 were send to the TOE. Also a higher load was analysed by sending a larger number of IP packets to the TOE. A number of evaluator test cases use the direct management interfaces of the TOE to verify that the TOE only allows an administrator to change management options.

Conclusion

The test results fulfil the requirements of ATE_IND.2.

7.3 Evaluator Penetration Testing

TOE Test Configuration

All configurations of the TOE being intended to be covered by the current evaluation were tested. The description of the required non-TOE hardware, software and firmware is described in section 1.2.2 of [6]. A stand-alone PC with an Intel Core i5 CPU clocked with 2.53GHz, 4GB RAM, operating system Ubuntu GNU/Linux 10.04.1 was used to virtualize the complete testing network environment including the TOE. Two Debian GNU/Linux systems, 'Source' and 'Destination' were installed and used in the testing network environment, each with three virtual interfaces. The TOE was provided by the developer and mounted on a virtual machine identical to the one used in the independent evaluator functional tests.

Testing Approach

For the penetration tests the differential Firewall analysis method was used. In this method someone needs to be able to compare the traffic on the “outside” to the traffic on the “inside” in real-time and alert when this contradicts. Therefore two “monitoring” points must be placed logically in front and behind the packet filter. At the two monitoring points a sniffer is placed at which the network traffic is analysed. These monitoring points are the bridges “net-in” and “net-out” of the test network.

The sensor is placed on the “inside” to alert if traffic is detected and violating the firewall rules. In the operational environment of the TOE it is also possible that malicious or unintended traffic is coming from the inside of the network passing the TOE. It was tested that the packet filter responds to both network interfaces in the same way. Therefore the extensive testing of one interface was sufficient to prove if the TOE is resistant to penetration tests.

Attack Scenarios being tested

After the setup of the test environment the different attack scenarios were defined. These attack scenarios were mapped to test cases and executed in the test environment.

The following list gives a short overview about the attack scenarios which have been tested:

- Port scan with or without different source ports to detect open ports.
- Bypassing the packet filter with fuzzy generated TCP, UDP or ICMP packets.
- Using the publicly available change log to find vulnerabilities.
- Bypassing the packet filter with packets with an incorrect IPv4 or IPv6 header.
- Bypassing the packet filter with a flood attack with “syn” or fragmented packets.
- Bypassing the packet filter with packets with a spoofed source address.
- Manipulation of the log output by sending incorrect payload in packets.
- Manipulation of Neighbour Discovery Protocol (NDP) for IPv6 to cause a denial of service
- Bypassing the access rule checks.

SFRs penetration tested

Only direct attacks against the implementation of SFRs need to be considered. It can be assumed that the SFRs are implemented correctly and that they cannot be bypassed, deactivated or manipulated. The tested SFRs are listed in the following:

- FDP_IFF.1 Simple security attributes
- FAU_GEN.1 Audit data generation
- FMT_SMR.1 Security roles

The remaining SFRs were analysed, but not tested through penetration due to non-exploitability of the related attack scenarios in the TOEs operational environment.

Conclusion

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential enhanced basic was actually successful. Therefore the test results fulfil the requirements of AVA_VAN.3.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE test configuration is defined by “Astaro Security Gateway Packet Filter version V1.000-4” with the hash values for the eight binary parts of the TOE. These hash values are exactly the same as given in table 3 in chapter 2. Therefore the evaluated configuration and the configuration tested during evaluation are the same.

9 Results of the Evaluation

9.1 CC specific results

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.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2 augmented for this TOE evaluation.

The evaluation has confirmed:

● PP Conformance:	None
● for the Functionality:	Product specific Security Target Common Criteria Part 2 conformant
● for the Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

In addition, the following aspects need to be fulfilled when using the TOE:

- The user must not load any new modules into the kernel. In case a new module is loaded the TOE is no longer certified.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
NDP	Neighbour Discovery Protocol
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
PP	Protection Profile
SAR	Security Assurance Requirement

SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionalities
UDP	User Datagram Protocol
VPN	Virtual Private Network

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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 passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8]

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0696-2011, Version 1.03, 2011-05-20, Security Target Astaro Security Gateway V8 Packet Filter, Astaro GmbH & Co. KG

[7] Evaluation Technical Report, Version 1.2, 2011-05-23, Evaluation Technical Report (ETR) - Astaro Security Gateway V8 Packet Filter, SRC Security Research & Consulting GmbH (confidential document)

[8] Configuration list for the TOE, Version 0.96, 2011-04-07, Konfigurationsliste, Astaro GmbH & Co. KG (confidential document)

[9] Guidance documentation for the TOE, Version 0.95, 2010-04-07, Applikationsentwicklerhandbuch, Astaro GmbH & Co. KG

[10] Flaw remediation, Version 0.93, 2011-01-27, Beheben von Schwachstellen, Astaro GmbH & Co. KG

[8] specifically

- AIS 1, Version 13, 14 August 2008, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 10, Version 2, 18 December 2010, Durch das BSI zugelassene Auslieferungsverfahren
- AIS 14, Version 7, 3 August 2010, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 7, 3 August 2010, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	**Assurance Components**
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 8.1)

“Table 1 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 CC 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 augmented with extended assurance requirements.

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A:	Security Target provided within a separate document.
Annex B:	Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0696-2011

Evaluation results regarding development and production environment

The IT product Astaro Security Gateway V8 Packet Filter Version 1.000, secunet wall 2 packet filter Version 1.000 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 3 June 2011, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_FLR.2, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

a) Development Site

Astaro GmbH & Co. KG

An der RaumFabrik 33a, 76227 Karlsruhe, Germany

b) Data Centre

TelemaxX Rechenzentrum 3 – IPC3,

Auf der Breit 5a, 76227 Karlsruhe, Germany

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.