Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0792-2013

for

gateProtect Firewall Packet-Filtering-Core Version 10.3

from

gateProtect AG Germany

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-0792-2013

Packet Filtering Firewall

gateProtect Firewall Packet-Filtering-Core
Version 10.3

from	gateProtect AG Germany
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1

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, 21 February 2013

For the Federal Office for Information Security

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

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

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

[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

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

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 September 2011 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 website: 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 by the nations listed above.

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 gateProtect Firewall Packet-Filtering-Core, Version 10.3 has undergone the certification procedure at BSI.

The evaluation of the product gateProtect Firewall Packet-Filtering-Core, Version 10.3 was conducted by atsec information security GmbH. The evaluation was completed on 18 February 2013. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: gateProtect AG Germany.

The product was developed by: gateProtect AG Germany.

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,

[6] Information Technology Security Evaluation Facility

- the product is operated in the environment described, as 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 gateProtect Firewall Packet-Filtering-Core, Version 10.3 has been included in the BSI list of 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] gateProtect AG Germany
Valentinskamp 24
20354 Hamburg

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 gateProtect Firewall Packet-Filtering-Core Version 10.3. The TOE is the network information flow enforcing software component of the gateProtect Firewall v10.3 from gateProtect AG. The gateProtect Firewall v10.3 product is shipped in the form of a self-contained Linux-based appliance. The TOE contains, besides the Packet-Filtering Core implementing the Network Information Flow Control Policy, a configuration engine that simplifies the rule specification. Key security features are: network information flow control, audit and configuration of the network information flow control policy by configuration files.

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.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.2. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functions	Addressed issue
Network Information Flow Control	The Network Information Flow Control Policy is enforced by the TOE providing a filtering mechanism that is integrated into the networking stack of the underlying system. All packets flowing to, from or through the system are subject to this filtering mechanism. They are either passed on or dropped according to the policy.
Audit	All packets handled by the firewall are subject to a statistics gathering module that records connections and provides a log of all connections and connection attempts handled by the firewall. In addition to packet and connection oriented logging, reaching configured thresholds (quota limits) for connections will also generate audit events. Configuration changes are subject to audit record generation.
Configuration	The network information flow control can be modified by a configuration file in the TOE environment that the TOE uses to configure its runtime behavior. The default policy is to drop packets and only by configuring explicit policies packets can be transported to or through the firewall. The configuration encompasses the behavior of the Network Information Flow Control and the audit subsystem. Configuration changes are performed by editing a configuration file in the environment which is then read by the TOE via a parser and translated into the detailed rules for the enforcement component.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1.

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], chapter 3.

This certification covers the configurations of the TOE, as summarised in chapter 8. It is software only, accompanied by guidance documentation. The supported platforms for the evaluated configuration are GPA 250, GPA 400 and GPX 2500.

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:

gateProtect Firewall Packet-Filtering-Core, Version 10.3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1.	SW	ISO image: gp-x-utm-10.3-i386-CD-1.iso SHA-512 hash value: dc776746 74f6933e 4994d835 be1a3b8a fc1ffa34 0555d870 d1ff6136 4027758a 58d73e8e 500f2f53 1f4653df deda6f5846e54302 e2ba7e7d 9e0440f1 1fa43467	10.3	Download
2.	DOC	gateProtect Firewall v10.3 Packet Filtering Core Evaluated Configuration Guide [9] File-name: gP-V10-ECG.pdf SHA-512 hash value: 23392393 4d786636 97fbb03d 75b93775 6fc4d24a 754c9f37 d9cefdad a698b3dd c0675f42 37597908 fb41bfc8 c0e4606e 94f3bc98 e44f9460 5a9bd5d5 aea18757	1.1	Download
3.	DOC	Memo to Customer of gateProtect Firewall v10.3 Common Criteria Configuration	N/A	FAX (phone line)

Table 2: Deliverables of the TOE

Also part of the electronic delivery (download) but not part of the TOE is a tool called CreateUSBInstaller. It comes in two varieties, one for Linux and one for Windows, and can be used to turn the installer image into a bootable USB stick.

No	Type	Identifier	Release	Form of Delivery
1.	SW	CreateUSBInstaller (Linux): CreateUSBInstaller.zip SHA-512 hash value: 882e336e 83cf72c5 0019810b ae152978 828956a1 e2da3099 ed94ca2a b2b400df b57969ca 0fdc46b5 c9d03208 68202dcf 8999354d 56df879d 1d573787 013d8d27	N/A	Download

No	Type	Identifier	Release	Form of Delivery
2.	SW	CreateUSBInstaller (Windows): CreateUSBInstaller-win32.zip SHA-512 hash value: 6b13fe49 df2eb1b5 e2bb1e9e 7b5b09e0 3681e2a4 aaf10139 ebf67fab 1d067e67 1ff39d1e 8a18f3ca 4f331b16 1d11bc2e 111466c0 1c0ef629 5d6d9290 475a5143	N/A	Download

Table 3: Deliverables not part of the TOE

The gateProtect Firewall v10.3 product is shipped as a self-contained Linux-based appliance. The TOE is delivered separately. As integral software part of gateProtect Firewall v10.3 product, the TOE can nevertheless not be ordered standalone.

The ISO image containing the TOE is delivered electronically to the customer together with the installer and the user guidance documentation over the https-protected and access-controlled gateProtect web site (https://www.gateprotect.com/mygateprotect/). Integrity and authenticity of those items delivered is ensured by providing a document with the respective SHA-512 hashes (as listed in Table 2 and Table 3) over a separate trusted communication channel, i.e. via FAX (phone line) and requiring the customer to compute the hashes of the downloaded files and compare them with the hash values contained in the FAX.

In order to verify the installed version of the TOE the user can execute the command "cltool -d version" as described in the guidance documentation [9], section 2.7 and compare the output with the listing for the evaluated version as given in the guidance documentation. The information provided allows the consumer to clearly identify the TOE upon purchase and use.

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:

- Network Information Flow Control
- Audit
- Configuration

For more information on these issues, see Security Target [6], chapter 1.5.4.1.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats 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 IT-environment must provide logical and physical protection of the administrative access to the TOE.
- The administrative network access to the TOE must only use a dedicated port of the appliance and not any of the other available network ports.

- Authorised administrators are competent, non-hostile and are trained as to the establishment and maintenance of sound security policies and practices for the privileges they have been given.
- The underlying operating system must enable the authorised administrator to read the recorded audit trail.
- The TOE environment must protect configuration and other TSF data stored in files against any undetected unauthorised modification.
- The TOE and its underlying hardware must be protected from physical access by unauthorised personnel.
- The underlying hardware, firmware (BIOS and device drivers) and operating system functions must be working correctly and must not have undocumented security critical side effects on the functions of the TOE.
- All information must flow through the TOE.
- The IT environment provides reliable timestamps.

Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The enforcing components of the system, the Network Information Flow Control Subsystem (NIFC-Subsystem), are implemented via IPTables. The filtering modules are embedded in the network stack of the appliance's underlying Linux system. The key difference between a regular IPTables firewall and the gateProtect firewall product is the way the rule base is configured. Instead of having to manually specify many detailed rules for IPTables, the gateProtect Firewall v10.3 product works with high level descriptive rules that model communication relationships. The configuration loading and rule transforming parts, a configuration database and the enforcing kernel components are all part of the TOE together with the audit daemon.

Figure 1 in the ST [6] shows the structure of the TOE. The physical and logical network interfaces (If) provided by the Linux environment deliver packets to the Network Information Flow Control Subsystem (NIFC) which handles the information flow control decisions based on the configuration of the NIFC and on the packet header information. This happens for all packets arriving at the network interfaces, regardless of whether they are destined locally or are to be routed through. The "Rules" part in Figure 1 is implemented via IPTables.

The Network Information Flow Control Subsystem configuration is loaded by a configuration loader (cltool) that reads the supplied configuration file and passes it on to the configuration daemon (stated) that transforms the user rules into IPTables rules and manages the available configurations in a configuration database. The configuration daemon then uses the iptables-restore script to load and activate the required IPTables rules into the kernel. The Configuration Mechanism Subsystem (CFG) consists of the configuration loader (cltool) and the configuration daemon (stated).

Audit information including statistical data about the packet flow is provided by the packet filter. The configuration daemon provides audit information about configuration changes. The audit log daemons (ulogd, rsyslogd) gather that information and provide the audit log files on disk. A watchdog daemon (monit) monitors the available file space for the audit data and generates alerts via the log file and e-mail should a configured threshold be reached. These three modules comprise the subsystem for Logging and Auditing (LOG). The configuration for monit is provided via stated.

The visible interfaces to the TOE are the configuration file, the audit logs and the logical (and therefore also physical) network interfaces.

6 Documentation

The evaluated documentation [9] as outlined in table 2 (no. 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 test environment contains six virtual test machines. These test machines are used to send packets between at least two interfaces of the TOE and to provide a test result. The test result gets analysed by the "test master". The "test master" controls the test machines and sets up the firewall appliance (TOE). The tested firewall appliances are: GPA 250, GPA 400 and GPX 2500.

The TOE was installed and configured as defined in the Evaluated Configuration Guide [9] with additional software packages required for testing.

Testing Approach

The developer has specified and implemented test cases that cover all individual TSFI identified for the TOE. In addition to the mapping to the functional specification, the developer provided a mapping of TSFI to subsystems of the high-level design. This mapping shows that all subsystems are implicitly covered by test cases.

All automated test procedures provided by the developer have the same structure and are documented inline. The automated test procedures are setting up the prerequisites on all involved test machines and the TOE. After all prerequisites have been set and no error occurred, the test itself is executed. After the test run, the actual result is compared with the expected result. If those results are the same the test is assigned the verdict "PASS", otherwise "FAIL".

Conclusion

The evaluator has verified that developer testing was performed on hardware conformant to the ST [6]. The evaluator analysed the developer testing coverage and the depth of the testing by reviewing all test cases. The evaluator found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification as well as the subsystem/internal interfaces identified in the design documentation. The evaluator reviewed the test results provided by the sponsor for each hardware configuration and found them to be consistent with the expected test results according to the test plan.

7.2 Evaluator Independent Testing

TOE Test Configuration

The evaluator set up the test systems according to the documentation in [9]. The evaluator's configuration is therefore also consistent with the ST [6].

The automated tests were performed on the physical firewall appliances provided by the developer, namely GPA 250, GPA 400 and GPX 2500. The manual test cases were executed on the GPX 2500.

Testing Approach

The evaluator testing effort consists of two parts. The first one is the execution of the developer tests and the second is the execution of the tests created by the evaluator.

During the evaluator's review of the test cases provided by the developer, the evaluator gained confidence in the developer testing effort and the depth of test coverage in the developer supplied test cases. The analysis has shown a very wide coverage of the TSF, therefore the evaluator devised only a small number of test cases based on the following reasons:

- The test cases examine some of the security functions of the TOE in more detail than the developer-supplied test cases.
- The test cases cover aspects not included in the developer testing.

Conclusion

The test systems were configured according to the ST [6] and the instructions in the guidance documentation [9].

The evaluator determined that the test results for all appliances are consistent and that the results of the developer tests performed by the evaluator as well as his additional test cases are consistent with the expected results. All tests passed successfully.

7.3 Evaluator Penetration Testing

TOE Test Configuration

The evaluator used the same test environment that was used for the independent testing. The TOE was set up in the default configuration. For some tests, additional configuration settings were required, such as configuring the external TOE interfaces with IP addresses and add routing information on the test machines in the environment.

Testing Approach

The testing was performed by using the TOE network interfaces, i.e. the administrative interface and the external interfaces. The evaluator tested the information flow control, the logging and the configuration capabilities and focused on attacks against the TOE security objectives.

The following areas were investigated during the testing:

- accessing the administrative interface from an external interface using fake addresses,
- gaining information about the TOE from network traffic it sends on its own,
- identifying possible attack surfaces through port scans,
- bypassing the connection logging and

- investigating the effects of invalid configuration inputs.

Conclusion

None of the tests that were performed by the evaluator revealed any exploitable vulnerabilities of the TOE at the claimed attack potential Enhanced-Basic.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE is software only and is accompanied by guidance documentation. The items listed in Table 2 of this report represent the evaluated configuration. The following appliances are supported platforms for the TOE:

- GPA 250,
- GPA 400,
- GPX 2500.

The operating system used is Debian Linux 6.0. The platforms and operating system as listed above are not part of the TOE but required for the correct operation of the TOE.

The following network protocols are supported:

- IPv4, IPv6,
- ICMP, ICMPv6, UDP, TCP, ESP, AH.

The following features and functions of the gateProtect Firewall appliance may be used but are not part of the evaluated TSF:

- Management eGui to generate the configuration file,
- Deep Packet Inspection,
- VPN Support.

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 component ALC_FLR.1 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.1

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 cryptographic algorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and Notes for the Usage of the TOE

The document as outlined in table 2 contains 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 OSPs 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.

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

AH	Authentication Header
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
DAC	Discretionary Access Control

DOS	Denial Of Service
EAL	Evaluation Assurance Level
eGUI	ergonomic Graphic User Interface
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
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.

JSON - JavaScript object notation , a structured way to define objects

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-0792-2013, Version 1.0, 2013-02-08, gateProtect Firewall Packet-Filtering-Core v10.3 Security Target, gateProtect AG

[7] Evaluation Technical Report, Version 2, 2013-02-11, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[8] Configuration lists for the TOE:

Build Server Configuration Item List, 2012-12-12 (confidential document)

CIL for the git documentation repository, 2012-12-12 (confidential document)

CILs for all git source code repositories, 2012-12-10 (confidential document)

CIL for the x-utm repository, 2012-12-10 (confidential document)

SVN Configuration Item List, 2012-12-03 (confidential document)

[9] Guidance documentation for the TOE, Version 1.1, 2012-12-05, gateProtect Firewall Packet-Filtering Core v10.3 Evaluated Configuration Guide

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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
AGD:	AGD_OPE.1 Operational user guidance

Assurance Class	**Assurance Components**
Guidance documents	
	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.

This page is intentionally left blank.