Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0382-2007

for

GeNUScreen 1.0

from

GeNUA

Gesellschaft für Netzwerk- und UNIX-Administration mbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0382-2007

GeNUScreen 1.0

from

GeNUA

Gesellschaft für Netzwerk- und UNIX-Administration mbH

Common Criteria Arrangement

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

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL 4 augmented by ALC_FLR.2 - Flaw reporting procedures**

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

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

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

Bonn, 04 July 2007

The President of the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

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

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

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

---

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

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2 Recognition Agreements

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

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC. As of February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America.

The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

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 GeNUScreen 1.0 has undergone the certification procedure at BSI.

The evaluation of the product GeNUScreen 1.0 was conducted by Tele-Consulting security | networking | training GmbH. The Tele-Consulting security | networking | training GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

GeNUA
Gesellschaft für Netzwerk- und
UNIX-Administration mbH
Domagkstrasse 7
85551 Heimstetten

The certification is concluded with

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

This work was completed by the BSI on 04 July 2007.

The confirmed assurance package is only valid on the condition that

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

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

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

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-20.

The product GeNUScreen 1.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] GeNUA
Gesellschaft für Netzwerk- und
UNIX-Administration mbH
Domagkstrasse 7
85551 Heimstetten

B Certification Results

The following results represent a summary of

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

Contents of the certification results

1 Executive Summary

The TOE ist the firewall system GeNUScreen 1.0 developed by GeNUA Gesellschaft für Netzwerk- und UNIX-Administration mbH

The TOE consists of

1. several firewall components that work as network filters and encrypting gateways,
2. a central Management Server that is used to configure, administrate and monitor the firewall components.

The Management Server allows authorised administrators to configure filter rules and protection policies on the firewall components by use of a web-based graphical user interface (GUI) at the Management Server. It also enables authorised administrators to update the software on the firewall components. The GUI must be used from a trusted machine connected to the Management Server through a trusted network.

After installation, all communication between the Management Server and the firewall components is protected by Secure Shell (SSH) transforms against eavesdropping and modification (Please note that SSH is considered being outside the TOE scope).

The firewall components employ IPsec encryption and authentication to protect data flows between the subnets assigned to them by the authorised administrators. Please note that the key management protocol (IKE) used for the IPsec communication is not part of the TOE.

Management consists of definition/modification and transmission of firewall policies and security policies for network traffic. The GUI also allows transfer of audit data from the firewall components.

The IT product GeNUScreen 1.0 was evaluated by Tele-Consulting security | networking | training GmbH. The evaluation was completed on 27 June 2007. The Tele-Consulting security | networking | training GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

GeNUA
Gesellschaft für Netzwerk- und
UNIX-Administration mbH
Domagkstrasse 7
85551 Heimstetten

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL 4+ (Evaluation Assurance Level augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: ALC_FLR.2	Life cycle support – Flaw reporting procedures

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

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

The following SFRs are taken from CC part 2:

Security Functional Requirement	Addressed issue
FAU	**Security audit**
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FCS	**Cryptographic support**
FCS_COP.1 (IPSEC-AES)	Cryptographic operation
FCS_COP.1(IPSEC-HMAC)	Cryptographic operation
FCS_CKM.4 (IPSEC)	Cryptographic key destruction
FDP	**User data protection**
FDP_IFC.1 (FW)	Subset information flow control
FDP_IFF.1 (FW)	Simple security attributes
FDP_ITT.1 (IPSEC)	Basic internal transfer protection
FDP_IFC.1 (IPSEC)	Subset information flow control
FIA	**Identification and authentication**
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT	**Security Management**
FMT_SMF.1 (FW)	Specification of Management Functions
FMT_MSA.3 (FW)	Static attribute initialization

Security Functional Requirement	Addressed issue
FMT_MSA.3 (IPSEC)	Static attribute initialisation
FMT_SMF.1 (IPSEC)	Specification of Management Functions
FMT_SMF.1 (Gen)	Security management functions

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

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Addressed issue
FAU	**Security audit**
FAU_GEN.1EX	Audit data generation

Table 3: SFRs for the TOE, CC part 2 extended

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

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

Security Functional Requirement	Addressed issue
FDP	**User data protection**
FDP_ITT.1 (IKE)	Basic internal TSF data transfer protection
FDP_IFC.1 (IKE)	Subset information flow control
FDP_IFF.1 (IKE)	Simple security attributes
FDP_ITT.1 (SSH)	Basic internal TSF data transfer protection
FDP_IFC.1 (SSH)	Subset information flow control
FDP_IFF.1 (SSH)	Simple security attributes
FCS	**Cryptographic support**
FCS_CKM.1 (IKE-AES)	Cryptographic key generation
FCS_COP.1 (IKE-AES)	Cryptographic operation
FCS_CKM.1 (IKE-DH)	Cryptographic key generation
FCS_COP.1 (IKE-DH)	Cryptographic operation
FCS_CKM.1 (IKE-HMAC)	Cryptographic key generation
FCS_COP.1 (IKE-HMAC)	Cryptographic operation
FCS_CKM.1 (IKE-RSA)	Cryptographic key generation
FCS_COP.1 (IKE-RSA)	Cryptographic operation
FCS_CKM.4 (IKE)	Cryptographic key destruction
FCS_CKM.1 (SSH-AES)	Cryptographic key generation
FCS_COP.1 (SSH-AES)	Cryptographic operation

Security Functional Requirement	Addressed issue
FCS_CKM.1 (SSH-DH)	Cryptographic key generation
FCS_COP.1 (SSH-DH)	Cryptographic operation
FCS_CKM.1 (SSH-HMAC)	Cryptographic key generation
FCS_COP.1 (SSH-HMAC)	Cryptographic operation
FCS_CKM.1 (SSH-RSA)	Cryptographic key generation
FCS_CKM.4 (SSH)	Cryptographic key destruction
FCS_COP.1 (SSH-RSA)	Cryptographic operation
FMT	**Security Management**
FMT_SMF.1 (IKE)	Specification of Management Functions
FMT_MSA.2 (IKE)	Secure security attributes
FMT_MSA.3 (IKE)	Static attribute initialisation
FMT_SMF.1 (SSH)	Specification of Management Functions
FMT_MSA.2 (SSH)	Secure security attributes
FMT_MSA.3 (SSH)	Static attribute initialisation
FPT	**Protection of the TSF**
FPT_STM.1 (ENV)	Reliable timestamps

Table 4: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.4.

These Security Functional Requirements assigned to the TOE are implemented by the following TOE Security Functions:

TOE Security Function	Addressed issue
SF_AU.1	Audit record generation
SF_AU.2	Specification of audit record contents
SF_AU.3	Display of audit records
SF_DF.1	Network layer (IP) and transport layer (TCP/UDP/ICMP) based information flow protection as routers or bridges
SF_DF.2	Re-assebmling of fragmented IP-datagrams
SF_DF.3	Dropping of spoofed and source routed IP packets
SF_DF.4	IPsec protected communication between firewall comonents
SF_DF.5	Header modification to reduce susceptability of information flow against hijacking attacks
SF_AC.1	Management of network traffic filter rules and IPsec tunnels on the Management Server by authorised administrators
SF_AI.1	Successfull identifcation and authentication of administrator at the Management Server before he can perform any security function

Table 5: Security Functions

For more details please refer to the Security Target [6], chapter 6.1.

1.3 Strength of Function

The TOE's strength of functions is claimed 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6] chapter 6.2.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

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

Users (subjects) and assets which are used for the description can be found in the Security Target [6], chapter 3.1.

The following table reproduces the threats as they are defined in the Security Target, chapter 3.4. Please note that there are no Organisational Security Policies defined for the TOE.

Threat name	Threat definition
T.NOAUTH	A user might attempt to bypass the security functions of the TOE to gain unauthenticated access to resources in the protected networks.
T.SNIFF	A user outside the TOE might gain access to the sensitive data passing between the protected networks. Attack method is packet inspection of Internet traffic.
T.SELPRO	A user from inside or outside the networks protected by the TOE components might gain access to the TOE and read, modify or destroy security sensitive data on the TOE, by sending IP packets to the TOE and exploiting a weakness of the protocol used.
T.MEDIAT	A user might send non-permissible data from outside the protected networks through the TOE that result in gaining access to resources in protected networks which is not allowed by the policy. The attack method is construction of IP packets to circumvent filters.
T.MSNIFF	A user outside the TOE might gain access to the configuration or audit data passing between the Management Server and a firewall component. Attack method is packet inspection of Internet traffic.
T.MODIFY	A user outside the TOE might modify the sensitive data passing between the protected networks. Attack method is packet interception and modification of Internet traffic.
T.MMODIFY	A user outside the TOE might modify the configuration or audit data passing between the Management Server and a firewall component. Attack method is packet interception and modification of Internet traffic.

Table 6: Threats defined in the Security Target of the TOE

1.5 Special configuration requirements

To guarantee that all Firewall components are set up correctly and know each other's and the Management Server's public keys, the following procedure is required:

1. A secure network is set up with only the Management Server and the Firewall components on it.
2. The management server must be installed from CD. During installation, public/private key pairs are generated which are used later to identify and authorize the Administrator.
3. The administrator initializes his/her account with a non-guessable password.
4. The administrator uses the GUI to create configurations for all the Firewall components. The configuration includes the creation of public/private key pairs for the Firewall components for later authentication by the Internet Key Exchange (IKE) and Secure Shell (SSH) protocols.

5. The Firewall components are installed by PXE boot from the Management Server. Among other things, the process installs on each firewall component
   1. the authorised administrator's public key
   2. the individual Firewall component's public/private key pair
   3. all the public keys of all the firewall components with which the individual firewall component is configured to communicate directly.

1.6 Assumptions about the operating environment

The following table reproduces the assumptions that are defined in the Security Target, chapter 3.2.

Assumption name	Assumption definition
A.PHYSEC	Each component of the TOE is physically secure. Only authorised administrators have physical access to the TOE. This must hold for the Management Server and the Firewall components.
A.INIT	The TOE was initialised according to the procedure described in the guidance documentation.
A.NOEVIL	Authorised administrators are non-hostile and follow all administrator guidance; however, they are capable of error. They use passwords that are not easily guessable.
A.SINGEN	Information can not flow between the internal and external network, unless it passes through the TOE.
A.NOADDSERV	The Management Server is exclusively configured to manage the Firewall components. No incoming traffic from untrusted networks is allowed to the HTTP service on the Management Server.
A.NOFWSERV	The Firewall components are configured to accept no incoming connections except SSH-protected data from the Management Server, IPsec Key agreement protocol connections and IPsec connections initiated by IPsec Key agreement from other firewall components of the TOE.
A.TIMESTMP	The environment provides reliable timestamps.
A.ADMIN	Authorised Administrators using the GUI on the Management Server work in a trusted network directly connected to the Server.

Table 7: Assumptions defined in the Security Target of the TOE

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation

that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

GeNUScreen 1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Management Server Model: 200, 400, 600, or 800 (in accordance with the specification in ST 2.2.1)	N/A	Hardware
2	HW	Two or more firewall Components Model: 100C, 300S, 500S, 200, 400, 600, or 800 (in accordance with the specification in ST 2.2.2)	N/A	Hardware
3	SW	Management Server Installation CD GeNUScreen Version 1.0 Z	1.0 Patchlevel 0	CD-ROM
4	DOC	Administrator Guidance	2.D038	Paper document / CD-ROM

Table 8: Deliverables of the TOE

Please note that the procedure to verify the authenticity of the SW TOE parts is described in the administrator guidance. The hash values needed for this validation are:

MD5(ports39.tgz) = 16ac51a360c7df63a208d2448bf08eb2

MD5(etc39.tgz) = bcacdd62b8e2b5c12f9d7287b699752e

MD5(comp39.tgz) = 93bf28b0b888e3fdb4ef1965b173afad

MD5(center39.tgz) = d7ea32e814c8f61b6bc217729b12a354

MD5(base39.tgz) = f1ade146a54b742909297af4f5109ee1

SHA1(ports39.tgz) = fc402a22b98e950b088fce3fd9931ee9066cfe20

SHA1(etc39.tgz) = 7a7d14aafd27663f168293f49ecf70f677ab2601

SHA1(comp39.tgz) = d90af5def769558fd23910aca8050bc055462389

SHA1(center39.tgz) = 721ea2c7404a2437cad8c958ec9223ec87dc8593

SHA1(base39.tgz) = 45923e48d9679930d9e23fef8a4078901eadbcd8

RMD160(ports39.tgz) = ba61f987799dc190f60b54a885ead46eeedee007

RMD160(etc39.tgz) = 1e809f28105091293c1d203a9246a83988f961f5

RMD160(comp39.tgz) = 14e49b5e09dc3eaa3aef27d0137aab9ca181d48a

RMD160(center39.tgz) = 77b6b1eff4d86fc7ddf862c0391647d65d5e88a0

RMD160(base39.tgz) = a11fadca5284aa3e599d629b1ed841f8d10c82a6

The hash values for the validation of the guidance document (as contained in the directory /cdrom/) are:

MD5(handbuch.pdf) = 5280ae2511aa9b710b1d815154af8f33

SHA1(handbuch.pdf) = 50973dc1aa6df85247d94db9eb2b98a791c2a31c

RMD160(handbuch.pdf) = 9d14056ee647e5750a1506dc0b16bb9233b0ca11

3 Security Policy

There are five securtiy policies defined for the TOE. Two policies are explictly defined:

- FW-SFP: Data flow control policy (implemented by the security function SF_DF)
- IPSEC-SFP: IPsec protected communication between firewall components (implemented by the security function SF_DF)

All other policies are implictly defined and cover the following areas:

- Audit Policy (implemented by the security function SF_AU)
- Identification and Authentication Policy (implemented by the security function SF_IA)
- Security Management Policy (implemented by the security functions SF_AU, SF_DF and SF_AC)

A more detailed definition is provided by the definition of the SFRs as given in the Security Target [6] and in the Security Policy Modell as provided for the assurance component ADV_SPM.1 (confidential document).

4 Assumptions and Clarification of Scope

For a detailed description of the assumptions see chapter 1.6 of this report.

4.1 Usage assumptions

The assumptions A.PHYSEC, A.INIT, A.NOEVIL and A.ADMIN describe the assumed usage of the TOE.

4.2 Environmental assumptions

A.SINGEN, A.NOADDSERV, A.NOFWSERV and A.TIMESTMP describe the assumptions about the environment of use of the TOE.

4.3 Clarification of scope

The following table presents the security objectives which have to be fulfilled by the TOE environment to support the TOE to meet its security goals and to avert the threats:

Objective name	Objective definition
OE.PHYSEC	Those responsible for the TOE must assure that the Management Server and the Firewall components are placed at a secured place where only authorised people have access.
OE.INIT	Those responsible for the TOE must ensure that the initial configuration is performed according to the user guidance documentation. Helps to avert the threats: T.SNIFF, T.MSNIFF, T.MODIFY and T.MMODIFY
OE.SINGEN	Those responsible for the TOE must assure that the Firewall components provide the only connection for the different networks. Helps to avert the threat: T.MEDIAT
OE.NOADDSERV	The Management Server must be exclusively configured to manage the Firewall components. No incoming traffic from untrusted networks must be allowed to the administrative GUI on the Management Server. Helps to avert the threat: T.SELPRO
OE.NOFWSERV	The Firewall components must be configured to accept no incoming connections except SSH-protected data from the Management Server, IPsec Key agreement protocol connections from other Firewall components of the TOE and IPsec connections initiated by IPsec Key agreement. Helps to avert the threat: T.SELPRO
OE.CRYPTO	The IT environment must supply SSH authorization and SSH transport protection as defined in [RFC4253]. The IT environment must supply Internet key agreement and the necessary algorithms as defined in [RFC2409], [PKCS #1, v2.0], [RFC2104], [RFC3526], [RFC3602], [FIPS-180-2] and [FIPS-197]. Helps to avert the threats: T.MSNIFF and T.MMODIFY

Table 9: Security Objectives for the environment which contribute to the aversion of threats

Please note that the table above only contains those security objectives for the environment which are related to threats. Security objectives for the environment which are related to assumptions/OSP only have not been listed.

A detailed assignment which security objective for the environment is related to which threat can be found in the Security Target, chapter 8.2 as a written rationale.

5 Architectural Information

The TOE is the firewall system GeNUScreen 1.0 developed by GeNUA Gesellschaft für Netzwerk- und UNIX-Administration mbH

The TOE consists of

1. Several (at least two) firewall components that work as network filters and encrypting gateways,
2. a central Management Server that is used to configure, administrate and monitor the firewall components.

The Management Server allows authorised administrators to configure filter rules and protection policies on the firewall components by use of a web-based graphical user interface (GUI) at the Management Server. It also enables authorised administrators to update the software on the firewall components. The GUI must be used from a trusted machine connected to the Management Server through a trusted network.

After installation, all communication between the Management Server and the firewall components is protected by Secure Shell (SSH) transforms against eavesdropping and modification (Please note that SSH is considered being outside the TOE scope).

The firewall components employ IPsec encryption and authentication to protect data flows between the subnets assigned to them by the authorised administrators. Please note that the key management protocol (IKE) used for the IPsec communication is not part of the TOE.

Management consists of definition/modification and transmission of firewall policies and security policies for network traffic. The GUI also allows transfer of audit data from the firewall components.

Core functionality

As core functionality the TOE offers a flexible and secure operating system with a TCP/IP-stack, routing functionality, packet filtering and cryptographic functionality which can be employed in a variety of different usage scenarios.

Functionality of the GeNUScreen component

- Statefull packet filter
- IPsec gateway
- Bridging (level-2) packet filter

Functionality of the GeNUCenter Management System

- Central firewall management
- Central logging station
- Central status monitor

On the abstraction layer of the high-level design the two TOE components are defined by the following subsystems:

- Subsystems of the firewall component: IPsec Code, network filter, service programs, audit.
- Subsystem of the Management component: WebGUI and backend daemon.

6 Documentation

The following guidance documentation is provided together with the TOE:

“GeNUScreen Installations- und Konfigurationshandbuch, ", [8]

This document contains all necessary instructions for correct installation and configuration of the TOE.

7 IT Product Testing

The test platform was set up by the developer according to the ST and all relevant guidance, ensuring that the evaluated configuration as defined in the ST was tested. The developer test scripts were performed successfully on the evaluated configuration of the TOE. Complete coverage was achieved for all the TOE security functions as described in the functional specification. The overall test depth of the developer tests comprises the high-level design subsystems as required for the assurance level of the evaluation.

The test scripts provided by the developer have been successfully repeated by the evaluation facility. The achieved test results matched the expected results as documented by the developer in the developer test documentation.

Furthermore, a set of independent penetration tests has been performed by the evaluation facility, without being able to compromise the TOE in the intended environment.

8 Evaluated Configuration

The Target of Evaluation (TOE) is called: GeNUScreen 1.0

It consists of the deliverables as outlined in chapter 2 of this report.

For installing the TOE a special procedure has to be followed. It is described in the user guidance documentation of the TOE [8] and summarised in chapter 1.5 of this report.

Please note that all information contained in the Security Target [6] and the guidance documentation [8] have to be followed in order to set-up, configure and use the TOE in a secure manner conformant to the evaluated configuration.

9 Results of the Evaluation

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

The evaluation methodology CEM [2] was used for those components identical with EAL4 and ALC_FLR.2.

The verdicts for the CC, Part 3 assurance components (according to EAL 4 augmented by ALC_FLR.2 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS

Assurance classes and components		Verdict
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Independent vulnerability analysis	AVA_VLA.2	PASS

Table 10: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL 4 augmented by ALC_FLR.2 - Flaw reporting procedures.
- The following TOE Security Functions fulfil the claimed Strength of Function: Security Function SF_AI.1 (Authentication and Identification)

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for the TOE Security Function SF_DF.4 (cryptographically protected communication between firewall components).

The results of the evaluation are only applicable to the TOE GeNUScreen 1.0 as outlined in chapter 2 of this report.

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

10 Comments/Recommendations

The guidance document [8] and the Security Target [6] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

None.

12 Security Target

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

13 Definitions

13.1 Acronyms

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

13.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Bibliography

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

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

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

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

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

[6] Security Target BSI-DSZ-0382-2007, GeNUScreen 1.0 Security Target Version 431, 11.06.2007, GeNUA mbH

[7] Evaluation Technical Report, Version 2, 27.06.2007, Evaluationsbericht BSI-DSZ-CC-0382 zu GeNUScreen 1.0 der GeNUA mbH durch Tele-Consulting GmbH (confidential document)

[8] GeNUScreen Installations- und Konfigurationshandbuch, Version 1.0 Z, Ausgabe 25.06.2007, Revision: build.2.D038

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

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

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

plus one of the following:

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

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

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

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

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

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

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

CC Part 3:

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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