Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0219-2007

for

netfence firewall
Version 3.0-2

from

phion information technologies GmbH

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-0219-2007

netfence firewall
Version 3.0-2

from

phion information technologies GmbH

Common Criteria Arrangement
for components up to EAL4

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) extended by advice of the Certification Body for components beyond EAL4 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 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL 4 augmented by** **AVA_VLA.3 – Moderately resistant** **ALC_FLR.1 – Basic flaw remediation**

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

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

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

Bonn, 08 March 2007

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

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

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

Preliminary Remarks

Under the BSIG1 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

Part A: Certification

Part B: Certification Results

Part C: Excerpts from the Criteria

A Certification

1 Specifications of the Certification Procedure

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

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

---

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

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

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

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

2 Recognition Agreements

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

2.1 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

This evaluation contains the components AVA_VLA.3 and ALC_FLR.1 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-components of these assurance families are relevant.

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 Netfence firewall, Version 3.0-2 has undergone the certification procedure at BSI. The evaluation of the product Netfence firewall, Version 3.0-2 was conducted by Tele-Consulting GmbH. The Tele-Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

phion information technologies GmbH
Eduard Bodem Gasse 1
A-6020 Innsbruck, AUSTRIA

The certification is concluded with

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

This work was completed by the BSI on 08 March 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-18.

The product Netfence firewall, Version 3.0-2 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] phion information technologies GmbH
Eduard Bodem Gasse 1
A-6020 Innsbruck, AUSTRIA

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	3
2	Identification of the TOE	8
3	Security Policy	9
4	Assumptions and Clarification of Scope	9
5	Architectural Information	10
6	Documentation	11
7	IT Product Testing	11
8	Evaluated Configuration	13
9	Results of the Evaluation	13
10	Comments/Recommendations	15
11	Annexes	15
12	Security Target	15
13	Definitions	15
14	Bibliography	17

1 Executive Summary

The netfence firewall system allows to control IP traffic between different networks and in particular from and to the internet. The system controls IP traffic between network nodes located in separated networks. The firewall system acts as an IP datagram router that controls datagram flow according to a configurable security policy which allows regulation of all IP protocols. To this end the product provides an Application Controlled Packet Forwarder (ACPF) as well as a Transparent Application Proxy (TAP).

The Application Controlled Packet Forwarder acts on IP packets (datagrams). For each datagram a decision based upon the configured firewall rules is made to control traffic between nodes. If the carried network protocol allows assignment of datagrams to sessions (e.g. TCP or UDP pseudo sessions) a state of these sessions is kept (stateful) and is taken into account in the decision process.

The Transparent Application Proxy controls data streams (TCP) from one network node to another. Based on the address (IP-Address and Port Number) of the initiating node (source) and the responding node (destination) establishments of such data streams can be allowed or denied as seen fit by the firewall ruleset. The system acts as an endpoint for the source node and as an initiator for the destination, controlling and analysing the flow and its content.

For each of these two transport methods (ACPF and TAP) two operation modes, inbound mode and outbound mode, are provided. The inbound method is provided to shield protected network nodes from TCP-SYN attacks performed across the TOE which aim at resource exhaustion of the protected node or nodes. To this end the TOE will first expect the three-way TCP handshake with the inititiating source node to be completed before attempting to connect the protected target network node. In outbound mode an incoming TCP-SYN packet is immediately passed on to the target network node.

The IT product Netfence firewall, Version 3.0-2 was evaluated by Tele-Consulting GmbH. The evaluation was completed on 30 January 2007. The Tele-Consulting GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

phion information technologies GmbH
Eduard Bodem Gasse 1
A-6020 Innsbruck, AUSTRIA

[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 4 augmented by AVA_VLA.3 and ALC_FLR.1. The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: AVA_VLA.3	Vulnerability assessment – Moderately resistant
+: ALC_FLR.1	Life cycle support – Basic flaw remediation

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_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FDP	**User data protection**
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FIA	**Identification and authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action
FMT	**Security Management**

Security Functional Requirement	Addressed issue
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on Security Roles
FPR	**Privacy**
FPR_PSE.1	Pseudonymity

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

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.

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

Security Functional Requirement	Addressed issue
FPT	**Protection of the TSF**
FPT_STM.1	Reliable time stamps

Table 3: 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.

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

- Security Administration
- Identification and Authentication
- Information Flow Control
- Privacy
- Security Audit

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 'high' (SOF-high) for specific functions as indicated in the Security Target [6, chapter 8.2.3].

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

The Security Target [6] describes the following threats to be countered by the TOE:

- **T.NOAUTH**: An unauthorised human user may attempt to bypass the security of the TOE so as to access and use security functions provided by the TOE.
- **T.ASPOOF**: An unauthorised user may carry out spoofing in which information flows through the TOE into the connected network by using a spoofed source address for TCP connections. An unauthorised user may carry out spoofing in which information flows through the TOE into the connected network by using a spoofed source address for all IP protocols for which a reverse routing path check from the TOE back to the source address yields a network device of the TOE other than the one the request from the source arrived on.
- **T.MEDTF**: An unauthorised user may send impermissible network information through the TOE which results in the exploitation of resources on a protected network.
- **T.PRIVACY**: A user may send information to the TOE and may analyse information received from the TOE to determine real IP addresses of external IT entities (network nodes such as hosts providing services or access to other networks) on the internal and demilitarized zone networks based on information extracted from received IP protocol headers. He may gain information about the IP addresses or TCP stacks used by the network nodes on the internal or demilitarized zone networks or about the topology of the protected networks. Retrieved information could be used by the user to optimise an attack strategy on network nodes within the protected networks.
- **T.NODETECT**: An unauthorised user may continually attempt to bypass the TSP without detection in order to successfully send data through the TOE.

The following security policies have to be met by the TOE as described in the Security Target:

- **P.ROLE**: The TOE must be able to distinguish between a root administrator with unrestricted management access, administrators with read/write permissions and administrators with read-only permissions.
- **P.AUDACC**: Users must be accountable for the actions that they conduct.

1.5 Special configuration requirements

For using the evaluated configuration of the TOE, the following physical components are needed:

- **Firewall**: Intel x686 compatible PC with at least 128 MB of memory, 4 GB Hard Disk, CDROM for installation, 1.44 MB Floppy disk drive for installation and 2 Network interfaces. The operating system used is Linux with Kernel Version 2.4.
- **Workstation for remote management**: Intel x86 compatible PC with 128 MB of memory, 4 GB Hard Disk, CDROM for software installation, 1.44 MB Floppy disk drive for preparation of firewall installation, 1 Network interface. As operationg system Windows NT4.0 (Service Pack 6a or newer), 2000 or XP is needed. Phioni (for installation or recovery purposes only) and Phiona remote administration software have to be installed.

1.6 Assumptions about the operating environment

The following assumptions about the environment of the TOE are made:

- **A.MEDEXP**: Potential threat agents attempting to attack the TOE are considered to be of a moderate attack potential. This incorporates familiarity with internet protocols, firewall principles and design, information published about the TOE, as well as tools and techniques for firewall penetration testing.
- **A.NOEVIL**: Administrators are non-hostile, competent, trained, and follow all administrator guidance.
- **A.ONEWAY**: Information cannot flow between networks connected to the netfence firewall unless it passes through the netfence firewall.
- **A.PHIONA**: After the netfence firewall has been installed, administrators use a Management Workstation to administrate it, not the system console.
- **A.PHYSEC**: The netfence firewall is operated in a physically secure environment which prevents access from unauthorised users.
- **A.WSSEC**: The Management Workstation is operated in an environment which is free of malicious software (trojan horses, etc.)
- **A.TIME**: The underlying operating system provides reliable time information to 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:

Netfence firewall, Version 3.0-2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Phion Netfence firewall	Version 3.0-2	CD ROM
2	SW	Linux Operating System	Kernel Version 2.4	CD ROM
3	DOC	Administrator Guidance	Rev.1.17	CD ROM
4	DOC	Start-up and Installation Guidance	Rev 1.10	CD ROM

Table 4: Deliverables of the TOE

All listed parts were delivered on 1 CD-ROM.

The user is able to verify the authenticity of the delivered TOE. The procedure is described in detail in the guidance documentation. At the phion website https://secure.phion.com/ the customer will find the actual guidance documentation, application phioni.exe and an MD5 checksum (CD-ID) of the TOE. The valid checksum of the TOE is:

64:c2:5f:99:05:72:47:38:f2:ba:a3:ee:a1:c7:3d:de

3 Security Policy

The netfence firewall system acts as an IP datagram router that controls datagram flow according to a configurable security policy which allows regulation of all IP protocols.

Therefore it provides mechanisms for controling and analysing the information related to security relevant activities and for the protection of user data. Management functionality is also provided, as well as mechanisms for identification and authentication.

The security policy of the TOE is definded by the following TOE security functional requirements:

- SFR components of the class FAU define the mechanisms for the security audit.
- SFR components of the class FDP define the mechanisms for the protection of user data.
- SFR components of the class FIA define the mechanisms for identification and authentication.
- SFR components of the class FMT define the management functions the TOE provides.
- SFR components of the class FPR define the mechanisms to provide privacy.

4 Assumptions

The security aspects of the environment in which the TOE is expected to be used are described in terms of assumptions. The assumptions for the environment are divided into assumptions about the intended usage of the TOE and assumptions about the environment the TOE is going to be used in.

4.1 Usage assumptions

- **A.MEDEXP**: Potential threat agents attempting to attack the TOE are considered to be of a moderate attack potential. This incorporates familiarity with internet protocols, firewall principles and design, information published about the TOE, as well as tools and techniques for firewall penetration testing.
- **A.NOEVIL**: Administrators are non-hostile, competent, trained, and follow all administrator guidance.

4.2 Environmental assumptions

- **A.ONEWAY**: Information cannot flow between networks connected to the netfence firewall unless it passes through the netfence firewall.
- **A.PHIONA**: After the netfence firewall has been installed, administrators use a Management Workstation to administrate it, not the system console.
- **A.PHYSEC**: The netfence firewall is operated in a physically secure environment which prevents access from unauthorised users.
- **A.WSSEC**: The Management Workstation is operated in an environment which is free of malicious software (trojan horses, etc.)
- **A.TIME**: The underlying operating system provides reliable time information to the TOE.

5 Architectural Information

The netfence firewall system controls IP traffic between network nodes located in separated networks. The firewall system acts as an IP datagram router that controls datagram flow according to a configurable security policy which allows regulation of all IP protocols.

The TOE is built of the following components:

- Netfence firewall service (TAP, ACPF): Software consisting of a collection of daemon processes that control packet forwarding and transparent proxying.
- Netfence kernel extensions (ACPF and Application Protection): Linux kernel modules that implement Application Controlled Packet Forwarding (ACPF) and support transparent proxying with additional security features (SYN Protection). The netfence firewall kernel extension is a loadable kernel module that adds firewalling functionality, used by the netfence firewall system, to the standard linux kernel.
- Netfence firewall base system (Visualization and Configuration): A collection of software modules allowing the administrator to control and analyse the status of the netfence system as well as that of the underlying Linux system. The netfence firewall base system also provides the interfaces for authorised rule set and system attribute management.
- Phiona (Remote administration client application): Software running on a Windows NT/2000/XP system allowing remote management of the netfence firewall. This involves firewall rule management, status visualisation as well as security audit evaluation.

- Phioni (Preinstallation setup): Software running on a Windows NT/2000/XP system allowing to preconfigure a netfence system for installation.

6 Documentation

For a listing of the documentation delivered with the TOE please refer to chapter 2 or chapter 14 of this report.

7 IT Product Testing

7.1 Developer Testing

The developer has provided test documentation (FAA2478) which identifies in chapter 1 the hardware of the used systems Alice (phion netfence firewall 3.0), Brain (Client, Red Hat Release 9), Barga (Client, Red Hat Release 9), Bob (Client / Administrator Workstation, Microsoft Windows XP SP2), and Acheron (Terminal Server / Administrator Workstation, Windows Server 2003). The test configuration consists of the TOE (firewall) with three network interface adapters. These are used to establish network connections to a management workstation and to test systems (barga, brain, bob) sending and receiving network traffic through the firewall.

The Security Target specifies seven assumptions about the environment of the TOE: Assumptions A.MEDEXP, A.NOEVIL, A.ONEWAY A.PHIONA, A.PHYSEC, A.WSSEC, and A.TIME. A.MEDEXP, A.PHYSEC, A.WSSEC and A.NOEVIL are not applicable to the test environment because access to the test equipment is properly set up and controlled by standard phion measures and procedures. Assumption A.ONEWAY is given in the test environment as figure 1 in the test documentation demonstrates. A.TIME is given in all TOE configurations because of the properties of the underlying operation system. Assumption A.PHIONA has been intentionally not fulfilled in the test environment in all cases to allow box access by a tool (cbad_test02) on a lower level interface than phiona or to allow to generate traffic via the local console which is blocked by the TSF.

The developer has elaborated a test suite of about 450 tests. To cope with dependencies within steps they have been arranged into test step assemblies. The description provided regarding the behaviour of the security functions varies between “minimal” (information flow control) to “detailed” (other security functions). Clear initial test conditions are assured by notes such as “Note that for these tests either a newly installed TOE must be used” or that “all existing administrators must be deleted before performing the test” or “any administrators or locks present from tests performed already have to be removed using phiona before continuing”. Cleanup activities are addressed in the test procedures by notes such as “IMPORTANT: restore the old hostname to the default settings after performing this test” or “IMPORTANT: restore the

old management IP and device to the default settings after performing this test". The test strategy makes intensive use of a pre-defined ruleset, which allows to ctivate and deactivate rules for specific tests. The test strategy also makes intensive use of test tools to support the tester in setting up the information flow for specific tests and to get access to lowerlevel interfaces which can not be stimulated directly by the management tool phiona. This allows to generate command sequences which are not admissible when using phiona. This is one of the means used by the developer to perform tests against the high level design specification. The majority of the tests focuses on testing the various modules controlling the information flow through and from/to the firewall.

The information provided shows that the expected test results are consistent with the actual test results.

7.2 Evaluator Testing

The evaluator has conducted independent testing by repeating developer tests and by performing additional tests.

The TOE system ("Alice") and two Linux test systems ("Barga" and "Brain") were provided by the developer. "Barga" and "Brain" were equipped with all test tools referenced in the developer's test documentation. The evaluator provided own equipment for use as management station (Windows XP SP2) and an additional MS-Windows based test systems (Windows XP SP1, not used for the documented tests). Alice were configured by the evaluator with three network interfaces. This configuration matches the configuration in the Security Target. Most of the tests were performed with Version 3.0-0.63, which differs from Version 3.0-0.64 only by the two guidance documents "Startup- and Installation Guidance" and "Administrator Guidance".

The version number of the TOE was changed from 3.0 to 3.0-2 during the evaluation. The change made on the operational TOE is only the change of the Version Number from 3.0-0.64 (this version of the TOE was included in the tests performed by the evaluation facility) to 3.0-2. Beside this change the software packages and documentation delivered with on CD 3.0-0.64 and 3.0-2 are identical.

The evaluator has devised penetration tests, building on the developer vulnerability analysis and its own vulnerability analysis.

The first type of penetration tests performed can be assigned to the category „testing against obvious vulnerabilities" (port scan, tool based vulnerability check etc.).

The evaluator devised a series of penetration tests to determine whether the suspected vulnerability regarding the double use of the TCP port 688 is existing.

The evaluator also performed a variation of the developer tests addressing unexpected input, invalid commands or parameters, data in unexpected context. These tests were performed using the developer tool test_cbad02.

It has to be considered that for this product type the boundary between functional tests and penetration tests is a bit fuzzy. This applies specifically for the tests of security function information flow control.

8 Evaluated Configuration

The evaluated version of the TOE is phion netfence firewall version 3.0-2 as described in the ST.

The TOE has to be set up in accordance to the guidance documentation ([8] - [9]) and the ST [6].

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. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 34]).

The verdicts for the CC, Part 3 assurance components (according to EAL 4 augmented by AVA_VLA.3 and ALC_FLR.1 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

Assurance classes and components		**Verdict**
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
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
Basic flaw remediation	ALC_FLR.1	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
Analysis and testing for insecure states	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Moderately resistant	AVA_VLA.3	PASS

Table 5: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by AVA_VLA.3 and ALC_FLR.1
- The following TOE Security Functions for identification and authentication fulfil the claimed Strength of Function:

The results of the evaluation are only applicable to the netfence firewall Version 3.0-2 as described 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 operational documents [8] - [9] 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

ACPF	Application Controlled Packet Forwarding
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
IP	Internet Protocol
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

UDP User Datagram Protocol

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-0219-2007, Version 1.9, 25.01.2007, of phion IT GmbH

[7] Evaluation Technical Report, Version 2, 29.01.207 (confidential document)

[8] phion netfence firewall 3.0 Administrator Guidance, Revision 1.17, 2006

[9] phion netfence firewall 3.0 Start-up and Installation Guidance, Revision 1.10, 2006

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.”