Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-006 CR Certification Report

Issue 1.0 1 November 2007

Thales Trusted Security Filter - TSF 101

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.0 13.09.2007

SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

Contents

Certification Statement

TSF101 is a filter between a secure and a non-secure IP network. The main purpose of the TSF101 is to filter a defined set of messages from the secure network to the non-secure network in a specific environment. Messages that do not comply with the specification of the filter are rejected.

The TSF101 with

Software version:

- 3AQ 21850 BAAA – 1.6

Hardware versions:

- 3AQ 21564 AAAA ICS5
- 3AQ 21564 AAAA ICS5A
- 3AQ 21564 AAAA ICS6
- 3AQ 21564 AAAA ICS6A
- 3AQ 21564 AAAA ICS6B
- 3AQ 21564 AAAA ICS7
- 3AQ 21564 AAAA ICS7A
- 3AQ 21564 AAAA ICS7B

has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 requirements of Evaluation Assurance Level EAL 5 for the specified Common Criteria Part 2 functionality when running on the platforms specified in Annex A.

Author	Arne Høye Rage Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	1 November 2007

1 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EWP	Evaluation Work Plan
ITSEF	IT Security Evaluation Facility
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SoF	Strength of Function
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

2 References

[1] Trusted Security Filter Security Target, 3AQ 21840 XAAA SCZZA Ed.4, 29 October 2007.

[2] Common Criteria Part 1, CCMB-2005-08-001, Version 2.3, August 2005.

[3] Common Criteria Part 2, CCMB-2005-08-002, Version 2.3, August 2005.

[4] Common Criteria Part 3, CCMB-2005-08-003, Version 2.3, August 2005.

[5] The Norwegian Certification Scheme, Sd 001E, Version 6.0, 02.07.2007.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2005-08-004, Version 2.3, August 2005.

[7] Common Criteria version 2.3 - EAL5 Methodology, Version 4, 03.11.2006.

[8] Evaluation Technical Report of the Trusted Security Filter – TSF 101, S-1833/20.06, issue 1.2, 31.10.2007.

[9] Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven) med endringer, sist ved lov av 21. desember 2001 nr. 117. ("Act relating to Protective Security Services").

[10] TSF Technical Manual with Trusted Facility Manual 3AQ 41202 ABAA EO Ed. 4, July 2007

[11] TSF 101 Software Installation Guide 3AQ 21850 XAAA BGZZA Ed. 2, 08. December 2006

[12] TSF 101 Requirement Specification 3AQ 21840 BAAA DXZZA Ed. 2, 23. November 2006

[13] TSF 101 Security Design – System description 3AQ 21901 BAAA DEZZA Ed. 6, 07. June 2007

[14] Rationale for OTA HW changes used in TSF 101 Product 3AQ 21840 XAAA FCZZA Ed. 2.2, 31. May 2007

3 Executive Summary

3.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of TSF101 with software version 3AQ 21850 BAAA – 1.6 and hardware versions 3AQ 21564 AAAA ICS5, -ICS5A, -ICS6, -ICS6A, -ICS6B, -ICS7, -ICS7A and –ICS7B to the Sponsor, Thales Norway AS, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the TSF Security Target [1] which specifies the functional, environmental and assurance evaluation requirements.

3.2 Evaluated Product

The version of the product evaluated was TSF101 and software version 3AQ 21850 BAAA – 1.6 and hardware versions 3AQ 21564 AAAA ICS5, -ICS5A, -ICS6, -ICS6A, -ICS6B, -ICS7, -ICS7A and –ICS7B.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Thales Norway AS.

The TOE hardware provides connection for audio devices, loudspeaker and lamps, and the Ethernet interfaces, but is used purely as a data filter between two IP based networks. In this configuration only the Ethernet interfaces and the alarm lamps and indicator lamps are used. All other interfaces are disabled.

The TOE software performs the following main functions: Routing, Firewall and Red/Black separation.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

An overview of the TOE's security architecture can be found in Annex B.

3.3 TOE scope

The scope of the TOE is limited to the Trusted Security Filter – TSF 101, comprising software and hardware. The TSF 101 is based on the same hardware as the certified Operator Terminal Adapter – OTA, but there have been some modifications. In the scope of the TSF 101 Security Target the TOE HW is used purely as a data filter between two IP based networks, and in this configuration only the Ethernet interfaces and the alarm lamps and indicator lamps are used. All other interfaces are disabled.

The scope of the evaluation comprises the TOE software and hardware and that the TOE fulfils its security functions as described in the TSF 101 ST [1] section 6.1.

The TEMPEST certification is not within the scope of the evaluation.

3.4 Protection Profile Conformance

The TSF 101 Security Target [1] does not claim conformance to any protection profile.

3.5 Assurance Level

The TSF 101 Security Target [1] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL 5 was used. Common Criteria Part 3 [4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [2].

3.6 Strength of Function

A Strength of Function (SOF) claim is not applicable for the TOE. There are no TOE security functions that are probabilistic or permutational.

3.7 Security Policy

There are no Organizational Security Policies or rules with which the TOE must comply.

3.8 Security Claims

The TSF 101 Security Target [1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2 [3]; use of this standard facilitates comparison with other evaluated products. An overview of CC is given in CC part 1 [2].

3.9 Threats Countered

The threats that the TOE counters are as follows:

- Classified information on a secure channel may be transferred to non-secure channels.
- Security-critical part of the TOE may be subject to physical attack that may compromise security.
- An attacker may send classified information from the secure to the non-secure network, by the use of data messages.
- Electromagnetic emanations may divulge classified information
- Authorised persons may perform unauthorised use of the system's applications and management system inside the operation site.

3.10 Threats Countered by the TOE's environment

All threats are countered by the TOE.

3.11 Threats and Attacks not Countered

All threats and attacks are countered.

3.12 Environmental Assumptions and Dependencies

The following assumptions are assumed to exist in the environment:

- The system comprising the TOE and the connected networks is installed in a physical protected area, minimum approved for the highest security level of information handled in the system.
- All TOE managers are trained in the correct use of the TOE.
- All TOE managers have a minimum clearance for the highest security level of information handled in the system, and is authorised for all information handled by the system.
- Only managers with special authorisation are allowed to do configuration and management of the system including TOE.
- The TOE is used between two LANs in a protected environment and is installed according to the installation guidelines for the TOE.

3.13 IT Security Objectives

The TOE IT security objectives in the TSF 101 ST [1] are as follows:

- If a hardware or software failure is detected in the TOE, the TOE shall raise a local alarm.
- The TOE shall have an audit log that can be viewed by a web browser on the secure network.
- The TOE shall perform statistics registration of messages handled by the filter and provide facilities to present them for the TOE manager.
- Classified information shall be prevented from being transmitted on non-secure channels.
- Security critical functions shall be tested by a combination of power-up tests, periodic tests and/or continuous tests.
- The firewall filter shall not be configurable.
- The IT environment shall be able to display the web page with the firewall statistics. The web server resides in the TOE.
- Special authorisation is required to grant access to handle TOE firewall statistics.

The last two are Environmental IT Security Objectives.

3.14 Non-IT Security Objectives

The TOE non-IT security objectives in the TSF101 ST [1] are met by procedural or administrative measures in the TOE's environment and are as follows:

- The TOE shall be sealed in such a way that it is easy to see that it has been opened/tampered with.
- TEMPEST evaluation and certification of the TOE is performed by NSM. This certification ensures that NO.TEMPEST is achieved.
- Only authorised persons shall be given physical access to the system comprising the TOE and the connected networks.
- Authorised managers of the TOE must ensure that the TOE firewall statistics and audit log are used and managed effectively. On particular, TOE firewall statistics and audit log should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future.

The last two are Environmental Non-IT Security Objectives.

3.15 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

- Security alarms FAU_ARP.1
- Audit data generation FAU_GEN.1
- Security audit review FAU_SAR.1
- Protected audit trail storage FAU_STG.1
- Complete information flow control FDP_IFC.2
- Simple security attributes FDP_IFF.1
- Illicit information flow monitoring FDP_IFF.6
- Management of security attributes FMT_MSA.1
- Static attribute initialization FMT_MSA.3
- Specification of Management Functions FMT_SMF.1
- Abstract machine testing FPT_AMT.1
- Failure with preservation of secure state FPT_FLS.1
- Passive detection of physical attack FPT_PHP.1
- TSF domain separation FPT_SEP.1
- Reliable Time Stamp FPT_STM.1

The IT environment is required to satisfy the following SFRs:

- Potential violation analysis FAU_SAA.1
- Audit Review FAU_SAR.1.Env
- Timing of identification FIA_UID.1
- Security roles FMT_SMR.1

3.16 Security Function Policy

The TOE has an information flow security function policy defined in FDP_IFC.2, FDP_IFF.1, FMT_MSA.1 and FMT_MSA.3. The information flow control provides flow control between the user interfaces and the secure and non-secure network and information flow control between the secure and non-secure network. The flow control rules are based on:

- All messages from the secure network to the non-secure network are filtered in a firewall.

3.17 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001 [5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT).

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the TSF 101 Security Target [1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [4] and the Common Evaluation Methodology (CEM) [6] against the EAL 5 assurance package defined in CC Part 3 [4]. Methodology used for EAL 5 is [7], listed in the reference section.

SERTIT monitored the evaluation which was carried out by the Secode Norge AS IT Security Evaluation Facility (ITSEF). The Task Start-up Meeting was held on 20. June 2006. Three progress meetings were held and SERTIT also conducted an inspection of the evaluation facility, where the evaluation work was examined. The evaluation was completed when the ITSEF submitted the final Evaluation Technical Report (ETR) [8] to SERTIT on 31 October 2007. SERTIT then produced this Certification Report.

3.18 General Points

The evaluation addressed the security functionality claimed in the TSF 101 Security Target [1] with reference to the assumed operating environment specified by the TSF 101 Security Target [1]. The evaluated configuration is specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

4 Evaluation Findings

4.1 Introduction

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 5 assurance package.

Assurance class	Assurance components	
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.3	Development tools CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.3	Semiformal functional specification
	ADV_HLD.3	Semiformal high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_INT.1	Modularity
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.2	Semiformal correspondence demonstration
	ADV_SPM.3	Formal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.2	Standardised life-cycle model
	ALC_TAT.2	Compliance with implementation standards
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: low level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_CCA.1	Covert channel analysis
	AVA_MSU.2	Validation of analysis

	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.3	Moderately resistant

The evaluation addressed the requirements specified in the TSF 101 Security Target [1]. The results of this work were reported in the ETR [8] under the CC Part 3 [4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

4.2 Delivery

The TOE is treated as CCI equipment, and is distributed according to the Norwegian regulation "Forskrift om informasjonssikkerhet" § 7-1 to § 7-45 to the "Act relating to Protective Security Services" [9]. The distribution is described in § 7-19. The evaluators have checked that the procedures for delivery of CCI material are used.

The TOE is sent by a courier or by other methods approved by NSM if it is sent abroad. If the TOE is not sent by courier the sender shall notify the receiver on how the TOE is sent and when it can be expected to arrive.

If the TOE is sent within Norway the TOE is handled as NATO CONFIDENTIAL. On receipt of the TOE, the user is recommended to check that the certified version has been supplied, and to check that the security of the TOE has not been comprised in delivery.

4.3 Installation and Guidance Documentation

The developer performs all installation, generation, and start-up. The evaluators examined the guidance documents, TSF 101 Technical Manual [10] and SW Installation guide [11], and determined that the steps necessary for secure installation, generation, and start-up are documented and that the procedures result in a secure configuration.

Furthermore all instructions and guidelines for the secure use of TOE are described in the TSF 101 Technical Manual [10]. No functions or interfaces are available to non-administrative users. Hence, specific user guidance for non-administrative users is not provided for the TOE.

A list of the guidance documents is given in annex A.

4.4 Misuse

Administrators should follow the guidance [10] and [11] for the TOE in order to ensure that the TOE operates in a secure manner. The guidance documents adequately describe all possible modes of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively administer and use the TOE's security functions, and to detect insecure states.

To prevent possible misuse of the TSF 101 firewall it is recommended to inspect the audit log and the filter statistics periodically. Further information can be found in the TSF 101 Technical Manual [8] chapter 10.

4.5 Vulnerability Analysis

The evaluators were satisfied that the developer's vulnerability analysis describes all obvious vulnerabilities and that it gives a rationale for why they are / are not exploitable in the intended environment for the TOE.

The Evaluators' vulnerability analysis was based on the visibility of the TOE given by the evaluation process.

The evaluators produced and conducted ten penetration tests on the basis of the developer's vulnerability analysis, and the evaluators produced and conducted four penetration tests based on their independent vulnerability analysis.

4.6 Developer's Tests

The developer has thoroughly tested all security functions of the TOE and the tests are divided into four parts:

- Hardware tests – where many tests are automatic tests performed during production of the HW. Many of these tests include the security functions, which are implemented in the hardware.
- Self tests – which are part of the implementation and are performed at start up and as supervision.
- System tests – which are performed on the actual version of both hardware and software.
- Integration tests – which are performed on the actual version of both hardware and software.

The developer has specified 17 different tests for testing of the security functions in the TOE.

4.7 Evaluators' Tests

The evaluation team decided to focus the testing on the error conditions in the following security functions:

- SF.Security.Alarm
- SF.Information.Flow.Control
- SF.Self.Test
- SF.Fail.Secure

- SF.Domain.Separation
- SF.Firewall.Statistics
- SF.Audit.Log

The only security function that was not selected for devised testing is SF.Passive.Protection, which describes that the TOE has a physical sealing.

For ATE_IND.2.2E, the evaluation team devised a test subset of six tests and produced test documentation.

For ATE_IND.2.3E, the amount of samples selected for testing by the evaluation team was 11 different tests, which is 65% of the developers testing effort.

The test subset is described in the ETR [8]. The test configuration is described in annex A.

5 Evaluation Outcome

5.1 Certification Result

After due consideration of the ETR [8], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that TSF101 with software version 3AQ 21850 BAAA – 1.6 and hardware versions 3AQ 21564 AAAA ICS5, -ICS5A, -ICS6, -ICS6A, -ICS6B, -ICS7, -ICS7A and –ICS7B meets the specified Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 5 for the specified Common Criteria Part 2 functionality, in the specified environment.

5.2 Recommendations

Prospective consumers of TSF101 with

Software version:

- 3AQ 21850 BAAA – 1.6

Hardware versions:

- 3AQ 21564 AAAA ICS5
- 3AQ 21564 AAAA ICS5A
- 3AQ 21564 AAAA ICS6
- 3AQ 21564 AAAA ICS6A
- 3AQ 21564 AAAA ICS6B
- 3AQ 21564 AAAA ICS7
- 3AQ 21564 AAAA ICS7A
- 3AQ 21564 AAAA ICS7B

should understand the specific scope of the certification by reading this report in conjunction with the TSF 101 Security Target [1]. The TOE should be used in accordance with a number of environmental considerations as specified in the TSF 101 Security Target [1].

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 3.3 "TOE Scope" and Section 4 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration, listed in Annex A.

Annex A: Evaluated Configuration

TOE Identification

The TOE is uniquely identified as:

Thales Trusted Security Filter (TSF101)

Software version:

- 3AQ 21850 BAAA – 1.6

Hardware versions:

- 3AQ 21564 AAAA ICS5
- 3AQ 21564 AAAA ICS5A
- 3AQ 21564 AAAA ICS6
- 3AQ 21564 AAAA ICS6A
- 3AQ 21564 AAAA ICS6B
- 3AQ 21564 AAAA ICS7
- 3AQ 21564 AAAA ICS7A
- 3AQ 21564 AAAA ICS7B

TOE Documentation

The supporting guidance documents evaluated were:

- TSF 101 ST [1]
- TSF 101 Technical Manual [10]
- SW Installation Guide [11]
- TSF Req Spec [12]
- Security Design Part 1 [13]

TOE Configuration

The following configuration was used for testing:

The TSF 101 consisting of hardware version 3AQ 21564 AAAA ICS5 and software version 3AQ 21850 BAAA – 1.6. The developer has provided a rationale [14] on why the hardware versions listed in 3.2 are interchangeable. This rationale is also enclosed as Appendix A in the ETR [8].

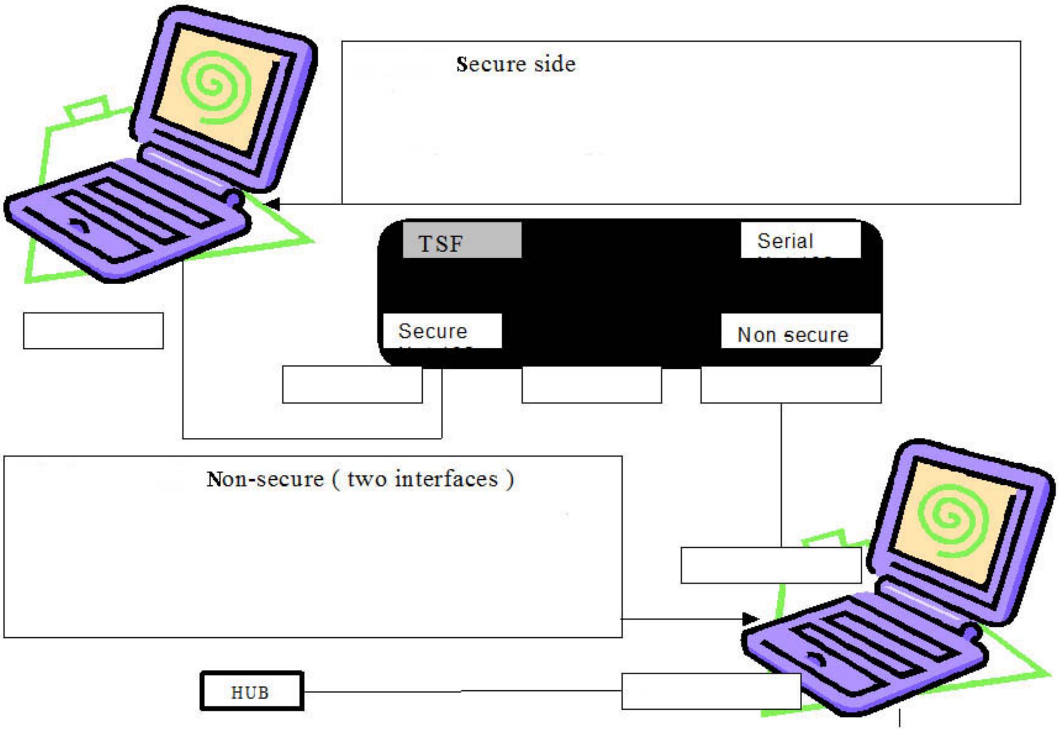

Figure 1 Test configuration

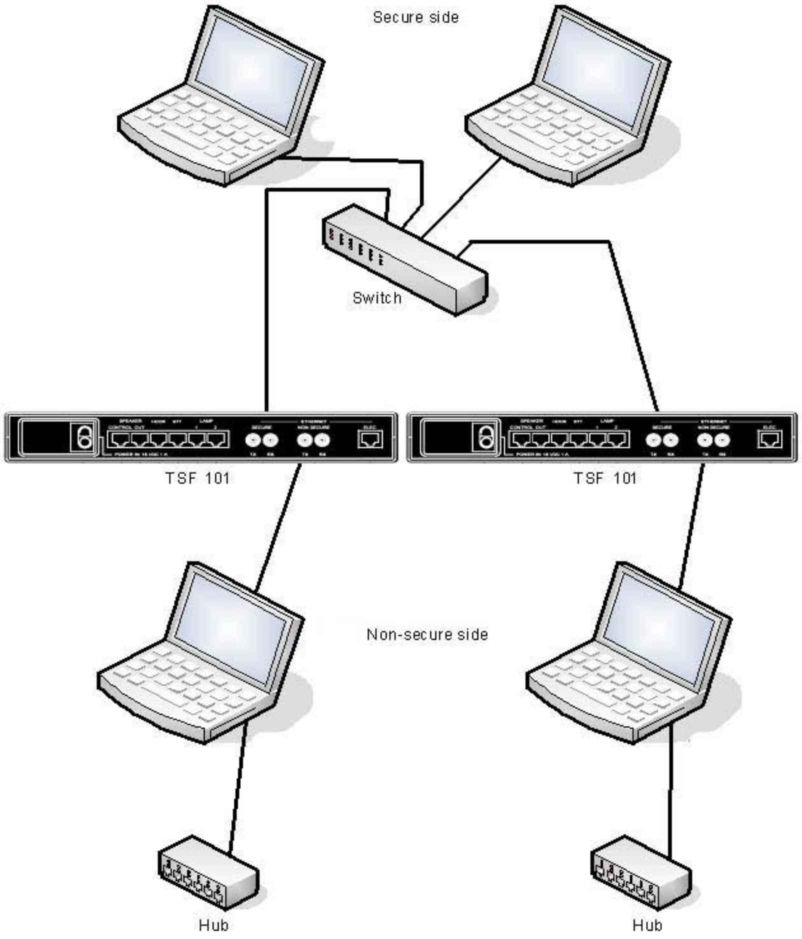

Figure 2 Penetration test configuration

The following test software was used:

- UDP sender (3AQ 21852)
- UDPListen2 (3AQ 21853)
- Message generator

For penetration testing of the TSF 101 the following software were used from a PC running Fedora Core release 6 (Zod):

- Nmap version 4.11
- Nessus deamon version 3.0.5.
- Nessus Client version 1.0.2
- Paros version 3.2.13
- Webscarab 20060718-1904
- Wireshark version 0.99.5
- Hping2 version 2.0.0-rc3

The definitions of the components used during evaluation/testing are:

2 PC (Secure):	Type:	Fujitsu Siemens, Lifebook E-Series
	Hardware:	Intel Pentium III, 698 MHz, 512 Mb RAM
	OS:	Windows XP Professional 2002, Service Pack 2
	SW:	ATOD message generator MSIFCsim2
2 PC (Non-secure):	Type:	Fujitsu Siemens, Lifebook E-Series
	Hardware:	Intel Pentium III, 698 MHz, 512 Mb RAM
	OS:	Windows XP Professional 2002, Service Pack 2
	SW:	UDPListen2
1 Laptop	Type:	HP Compaq nc8430
	Hardware:	Intel Centrino Duo, 2 GHz, 2 Gb RAM
	OS:	Fedora Core release 6 (Zod)
1 Ethernet network switch	Type:	Digital Data Communications FSW-0807TX Ver. 1A
1 Ethernet hub	Type:	3COM OfficeConnect Ethernet HUB 4C
1 Ethernet hub	Type:	3COM OfficeConnect DualSpeed HUB 5
2 Media converter	Type:	Allied Telesyn International MC101XL Fast Ethernet media converter

Annex B: Product Security Architecture

This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

The TOE HW provides connection for audio devices, loudspeaker and lamps, and the Ethernet interfaces.

Note that for TSF 101 the TOE HW is used purely as a data filter between two IP based networks, and in this configuration only the Ethernet interfaces and the alarm lamps and indicator lamps are used. All other interfaces are disabled.

The main function of the TOE HW is to perform red/black separation. The TOE uses an external AC/DC converter. All connectors intended to be handled by installation and maintenance are located at the rear end. The front end has indicator lamps providing information of the status of the TOE, the power and each of the Ethernet interfaces.

The TOE is connected to secure and non-secure LAN by use of 100 Mb/s Ethernet interface on fibre. It also has a 10/100 Mb/s electrical Ethernet interface. This interface gives access to the secure Ethernet, but is not in use for the TOE except for initial setting of the IP addresses of the TOE.

The TOE SW performs the following main functions:

- Routing

  The TOE will during normal operation have 2 different LAN connected; one secure LAN, and one non-secure LAN respectively, see Figure 1. This implies that TOE must be able to route IP packets.

- Firewall

  The firewall checks all messages from secure to non-secure domain. The firewall filter is not configurable, but is hard-coded for the specific IT environment, and it is identical in all TOEs.

- Red/black separation

  The secure (red) and non-secure (black) functions are separated using a combination of privilege levels and isolation of software tasks in different segments. Violation of segment boundaries is protected by the CPU and dedicated hardware.

The Trusted Security Filter – TSF 101 is a filter between a secure and a non-secure IP network. The system is designed to provide a continuous 24 hours operation 7 days a week. The main purpose of the TSF 101 is to filter a defined set of messages from the secure network to the non-secure network in a specific environment. Messages that do not comply with the specification of the filter are rejected.

Figure 3 shows the TSF 101 in its position as a data filter between two LAN networks

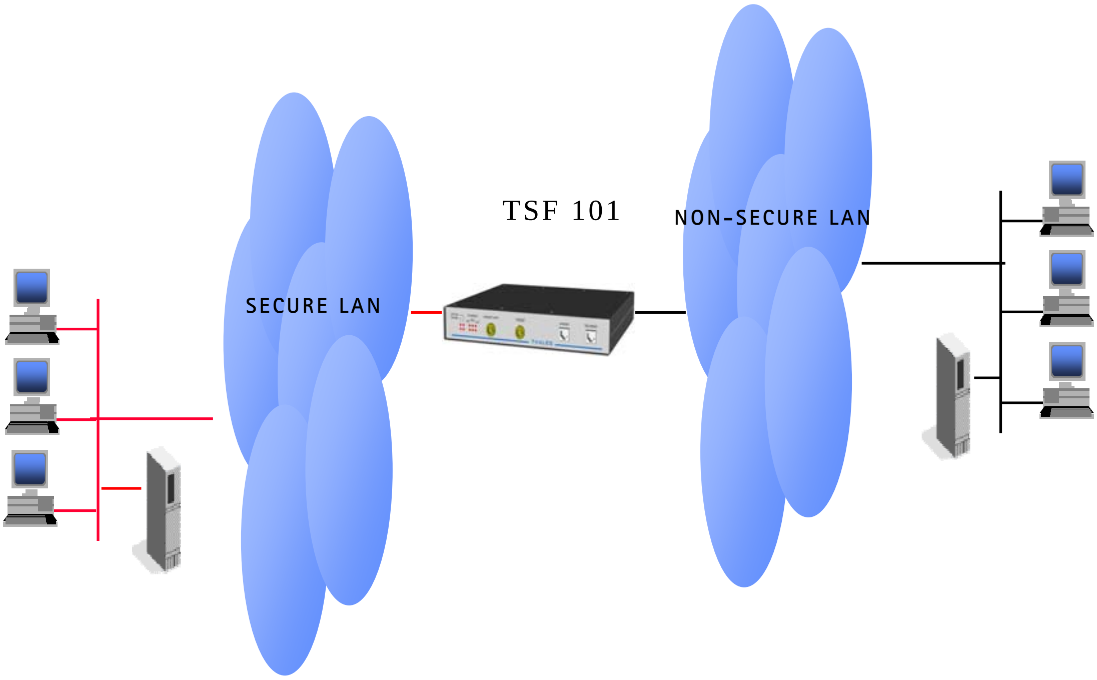

Figure 3 TSF 101 environment