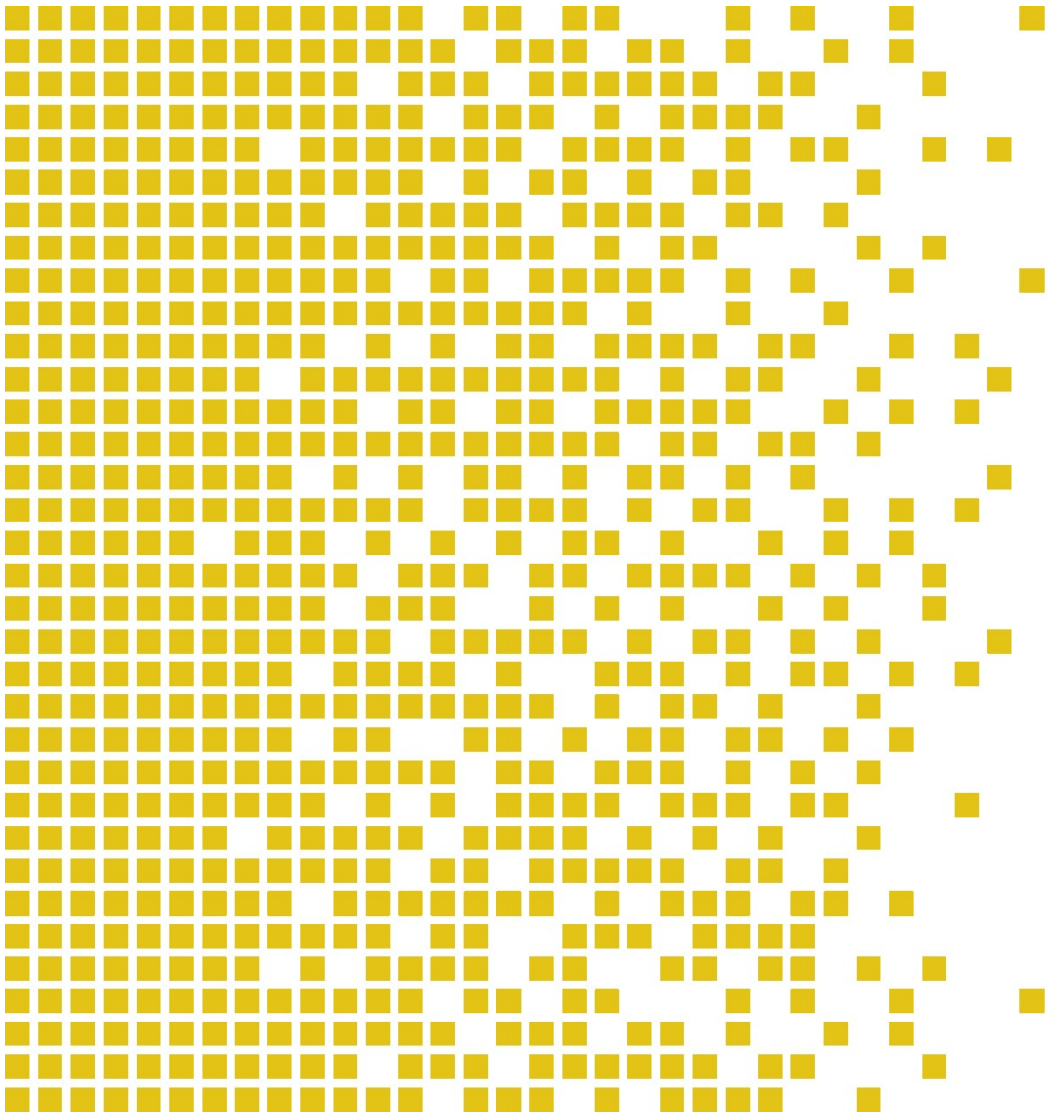
SERTIT-127 CR Certification Report

Issue 1.0 16 December 2025

Expiry date 16 December 2030

Trusted Security Filter (TSF) 401 SW 1.0.0



SERTIT, P.O. Box 814, N-1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The recognition under CCRA is limited to cPP related assurance packages or components up to EAL 2 with ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

Certification Statement

Trusted Security Filter (TSF) 401 allows secure data transfer between different security levels.

TSF 401 SW 1.0.0 has been evaluated under the terms of the Norwegian Certification Authority for IT Security [10] and has met the Common Criteria Part 3 (ISO/IEC 15408) [3] conformant components of Evaluation Assurance Level (EAL) 5 augmented with ALC_FLR.3 for the specified Common Criteria Part 2 (ISO/IEC 15408) [2] conformant functionality in the specified environment when running on the platforms specified in Annex A.

The evaluation addressed the security functionality claimed in the ST Lite [12] with reference to the assumed operating environment specified by the ST Lite [12]. The evaluated configuration was that specified in Chapters 1, 2 and 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.

Certifier	Øystein Hole, SERTIT
Date approved	16 December 2025
Expiry date	16 December 2030

1 Executive Summary

Prospective consumers are advised to read this report in conjunction with the ST Lite [12] which specifies the functional, environmental and assurance evaluation components.

The version of the product evaluated was TSF 401 SW 1.0.0.

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

The main purpose of the TOE is to inspect and filter data addressed from one security domain to another and only allow transfer of data that complies with the filter specification. The TOE has two separate and independent channels and is capable of filtering in both directions on the main channel, or operate as diode allowing all traffic in one direction and blocking all traffic in the opposite direction. The secondary channel can be used as diode or for interface redundancy.

Figure 1 illustrates the TSF 401 as a Cross Domain Solution (CDS) between networks.

Figure 1

No Protection Profiles are claimed.

Regarding the usage and the operational environment of the TOE, seven assumptions are made in the ST Public [12]. In order to counter seven threats as described in the ST Public [12], the TOE relies on the assumptions made. Details can be found in Chapter 3 Assumptions and Clarification of Scope.

The evaluation was performed by the ITSEF Nemko System Sikkerhet AS. The evaluation was performed in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in the document SD001E [10], as well as the Common Criteria (CC) Part 3 [3] and the Common Methodology for Information Technology Security Evaluation (CEM) [6].

The evaluation was performed at the assurance level EAL 5 augmented with ALC_FLR.3.

Nemko System Sikkerhet AS is an authorised ITSEF under the Norwegian Certification Authority for IT Security (SERTIT). Nemko System Sikkerhet AS is an accredited ITSEF according to the standard ISO/IEC 17025 for Common Criteria evaluation. The sponsor for this evaluation was Thales Norway AS.

The evaluation activities were monitored by the certification body. The security claims stated in the ST [11] was confirmed during the evaluation for the selected assurance level.

The basis for producing this Certification Report is the ST Lite [12] and the ETR [13].

2 TOE overview and Security Policy

Figure 2 shows the TSF 401 and its supporting tools. The supporting tools are outside the scope of the Common Criteria (CC) evaluation. The TOE is the TSF 401 main system with all SW, FW and HW modules. This includes the security filter mechanism, network services, internal management and management of filter files, trust anchors and certificates.

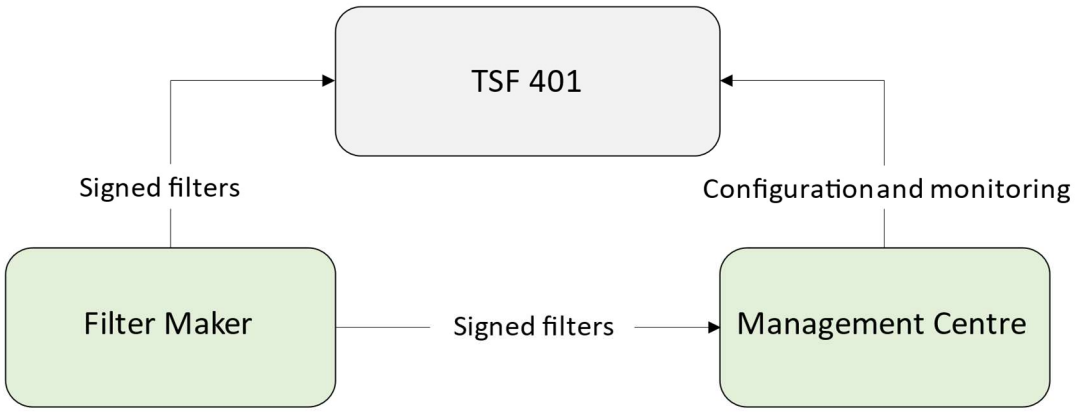


Figure 2

The TSF 401 is a CDS that provides secure data transfer between security domains of different security levels.

The Filter Maker is used for producing and signing the filter definition files.

The Management Centre is a central system for remote management and monitoring of TSF 401s.

The TSF 401 has two Ethernet interfaces on the High side and two Ethernet interfaces on the Low side. Filter function:

- One channel with fully configurable two-way filtering
  - Independent filtering each way (High to Low and Low to High)
  - Filters can be configured to work as a Diode allowing all traffic from Low to High and block all traffic from High to Low and vice versa.
- Two extra network interfaces that can be used in the following way:
  - For interface redundancy – active failover if link on the main interface fails; or
  - Configured as a diode.

The interfaces are called Red1 and Red2 on High side, and Black1 and Black2 on Low side.

Figure 3

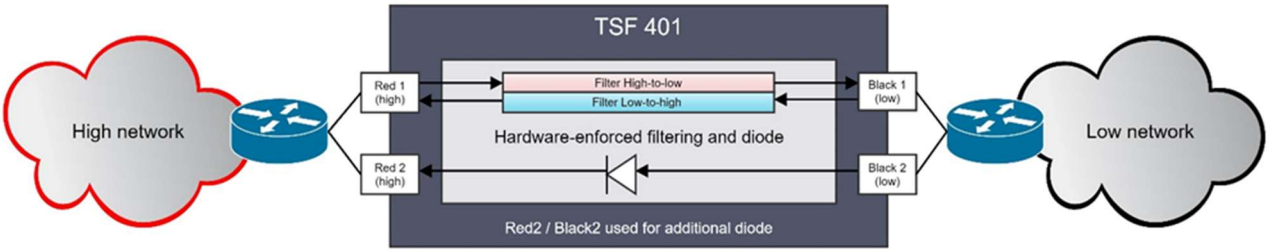


Figure 4

The default setting of the filter is “No traffic”, meaning that all traffic through the filter is blocked in both directions. This is the state of the system until a signed filter definition file is validated, installed and selected.

When a filter definition file is active, the TSF 401 only forwards data that complies with the filter specification. Non-compliant data is discarded and metadata is aggregated and available in the management centre.

The TOE provides the following main security features:

- Secure installation of filter definition files
- Secure storage of filter definition files
- HW enforced filtering mechanisms
- Protected audit log
- Endorsed cryptographic functions for disc encryption and SW/FW image protection
- Cryptographic Ignition Key (CIK)
- Secure certificate management and signature verification
- Secure boot, including self-tests of security critical functions
- Secure SW installation/update
- Software upgradeable from local USB or central management
- Tamper detection and response
- Zeroise switch
- Alarm and audit management from local HMI and central management

- Secure communication with a central management system
- Role based access control
- Complies with TEMPEST requirements according to SDIP-27 level A.

The filtering mechanism is implemented as a core filter enforcer that controls all data released through the filter from High to Low side and Low to High side. The filter enforcer, both offset-based and parser, is implemented in FPGA. The active filter can be selected from installed filter definition files during operation. A typical filter limits data exchange to a specified set of application messages. All other traffic/messages are stopped. The filter definition file is a set of rules for inspection of protocol parameters and message content. A filter allows only selected packets matching the rules to pass through the filter.

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following seven assumptions made regarding the usage and the operational environmental environment of the TOE are:

- PHYSICAL
- TRAINING
- CLEARANCE
- MAN_AUTHORISED
- USAGE
- ORGANIZATION
- HSP

For details on these assumptions, the reader is advised to look at chapter 3.2 in the ST Lite [12].

3.2 Threats Countered

The threats and threat agents met by the TOE are diverse and depend on where the TOE is deployed. The following seven threats are countered by the TOE:

- INFO_HIGH_LOW
- INFO_LOW_HIGH
- TAMPERING
- MISUSE
- TEMPEST
- UNAUTHORIZED_USE
- ILLEGAL_CONFIG

For details on these threats, the reader is advised to look at chapter 3.5 in the ST Lite [12]. The reader should also have a look at the description of the threat agents in chapter 3.4 in the ST Lite [12].

3.3 Threats Countered by the TOE environment

There are no threats countered by the environment.

3.4 Organisational Security Policies

During the evaluation of the TOE the following six Organisational Security Policies have been considered:

- ACCESS
- ACCOUNTABILITY
- IDENTIFICATION_AUTHENTICATION
- RESIST_MODERATE
- ANTI_TAMPER
- MAINTENANCE

All of the policies are compliant with applicable parts of Norwegian security policy [16] and NATO security policy [17]. The TOE Organizational Security Policies are detailed in Chapter 3.6 of the ST Lite [12].

4 Vulnerability Analysis and Testing

4.1 Vulnerability Analysis

The evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process. The search for publicly known vulnerabilities was conducted on 05 August 2025.

No exploitable vulnerabilities were found, but see chapter 7 in this report for recommendations for secure usage of the TOE.

4.2 Developer's Tests

The evaluation showed that the Developer has thoroughly tested the TOE Security Functionality Interfaces (TSFI) and TSF modules of the TOE, and the test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. The developer has tested all the TSF subsystems, all the SFR-enforcing modules, and all the SFR-supporting modules against the TOE design and the security architecture description.

4.3 Evaluators' Tests

The evaluators performed independent testing of a subset of the TSFIs and the TSF modules and verified that the TOE behaves as specified in the design documentation. Confidence in the developer's test results were gained by performing a sample of the developer's tests.

The evaluators devised penetration tests, based on the independent search for potential vulnerabilities and the security functions from the ST.

Testing was conducted in the week of 08-12 September 2025.

5 Evaluated Configuration

The evaluated TOE, as described in chapters 1, 2 and Annex A, is SW, FW and HW. The TOE is delivered as a physical unit with SW installed. Filters must be built and installed in order for the TOE to operate as intended.

Installation of the TOE must be performed completely in accordance with the guidance documents [14], [15] provided by the developer. The TOE should be used in the operational environment as specified in the ST Lite [12], as well as the guidance documents referenced in this chapter.

6 Evaluation Results

The evaluation addressed the requirements specified in the ST Lite [12]. The ITSEF reported the results of this work in the ETR [13] on the 12 February 2024.

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

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semiformal modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with implementation standards
	ALC_FLR.3	Systematic flaw remediation
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification

Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.4	Methodical vulnerability analysis

After due consideration of the ETR [13], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the certification team, SERTIT has determined that TSF 401 SW 1.0.0 meets the specified Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 5 augmented with ALC_FLR.3 for the specified Common Criteria Part 2 conformant functionality in the specified environment, when running on platforms specified in Annex A.

7 Recommendations

Prospective consumers of TSF 401 should understand the specific scope of the certification by reading this report in conjunction with the ST Lite [12]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST Lite [12].

The TOE should be installed and operated in accordance with the supporting guidance documentation [14], [15] included in the evaluated configuration.

Some recommendations were given by the evaluation team:

- If an open filter is available on TOE, it can be selected by the administrator which could lead to non-releasable information being transferred from High to Low.
- Filter description does not show before selecting the filter. If the administrator does not have an appropriate name for the filter, then an insecure filter may be selected.
- The menu had confirmation dialogue before select/delete with the default option set to “no” which makes it very hard to unintentionally select or delete the wrong filter. Due to not being able to see the filter on TOE, a good naming convention for the filters to separate them from each other should be encouraged.
- The design of the filter is very important to what information is being allowed through. Too strict filter would prevent legitimate traffic from passing through, while not strict enough would allow too much information to pass.

8 Security Target

The complete Security Target [11] used for the evaluation performed is sanitised for the purpose of publishing. The Public version (Security Target Lite [12]) is provided as a separate document. Sanitisation was performed according to the CCRA framework – ST sanitising for publication [7].

9 Glossary

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CDS	Cross Domain Solution
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
FPGA	Field Programmable Gate Array
FW	Firmware
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
ITSEF	IT Security Evaluation Facility under the Norwegian Certification Scheme
PP	Protection Profile
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirement
SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

10 References

[1] CC:2022, *Common Critera for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2022-11-001, Revision 1, CCRA, November 2022.

[2] CC:2022, *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2022-11-002, Revision 1, CCRA, November 2022.

[3] CC:2022, *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB-2022-11-003, Revision 1, CCRA, November 2022.

[4] CC:2022, *Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities*, CCMB-2022-11-004, Revision 1, CCRA, November 2022.

[5] CC:2022, *Common Methodology for Information Technology Security Evaluation, Pre-defined packages of security requirements*, CCMB-2022-11-005, Revision 1, CCRA, November 2022.

[6] CEM:2022, *Common Methodology for Information Technology Security Evaluation*, CCMB-2022-11-006, Revision 1, CCRA, November 2022.

[7] CCRA (2006), *ST sanitising for publication*, 2006-04-004, CCRA, April 2006.

[8] SOGIS Management Committee (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, Version 3.0, SOGIS MC, January 8th 2010.

[9] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, July 2nd 2014.

[10] SERTIT (2020), *The Norwegian Certification Scheme*, SD001E, Version 10.5, SERTIT, 03 December 2020.

[11] Security Target for TSF 401, Rev 3p003, 23 June 2025

[12] TSF 401 Security Target Lite, Rev 001, 28 November 2025

[13] Evaluation Technical Report Common Criteria EAL5+ Evaluation of Trusted Security Filter (TSF) 401 SW 1.0.0, version 1.1, 17 November 2025.

[14] Operator Manual TSF 401, Ed1p001

[15] Governance Manual TSF 401, Ed1p001

[16] Lov om nasjonal sikkerhet (Norwegian Security Act), LOV 2018-06-01 nr 24.

[17] C-M(2002)49, Security Within the North Atlantic Treaty Organisation (NATO), 17 June 2002.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

TSF 401 SW 1.0.0

Product ID: 3AQ 30600 AAXX

Refer to the manufacturer's documentation for additional information.

TOE Documentation

The supporting guidance documents evaluated were:

[a] Operator Manual TSF 401, Ed1p001

[b] Governance Manual TSF 401, Ed1p001

TOE Configuration

The system test is carried out in a test environment according to Figure 5, which shows the Hypervisor as a host for appliances on RED and BLACK side of the TSF 401:

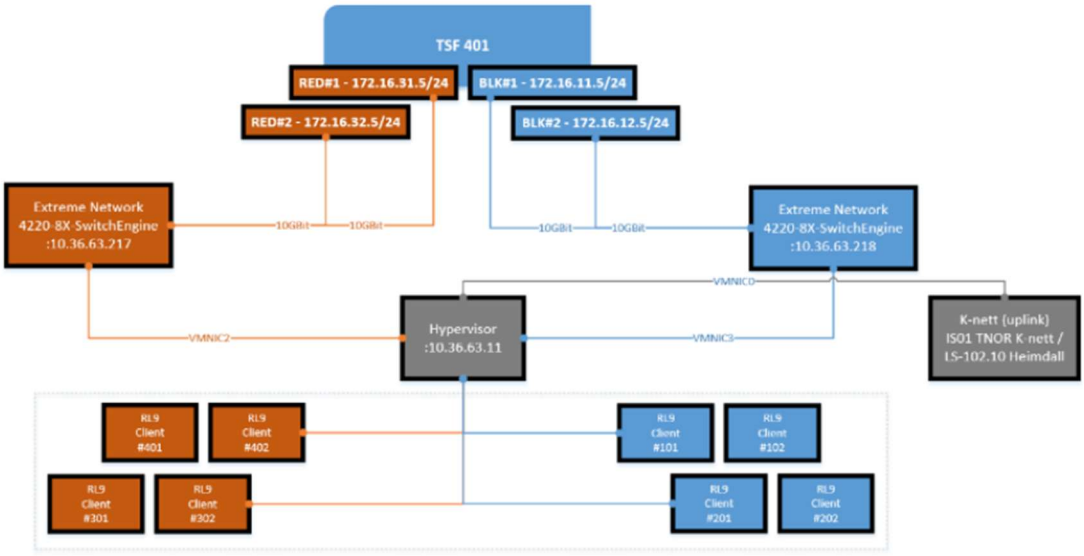


Figure 5

Figure 6 shows 8 end-systems, where 4 end-systems are indirectly connected to the first level on TSF 401, and where the other 4 end-systems are all behind routers. The idea behind this design is to test and verify that TSF 401 can handle larger networks that include routing and other network services.

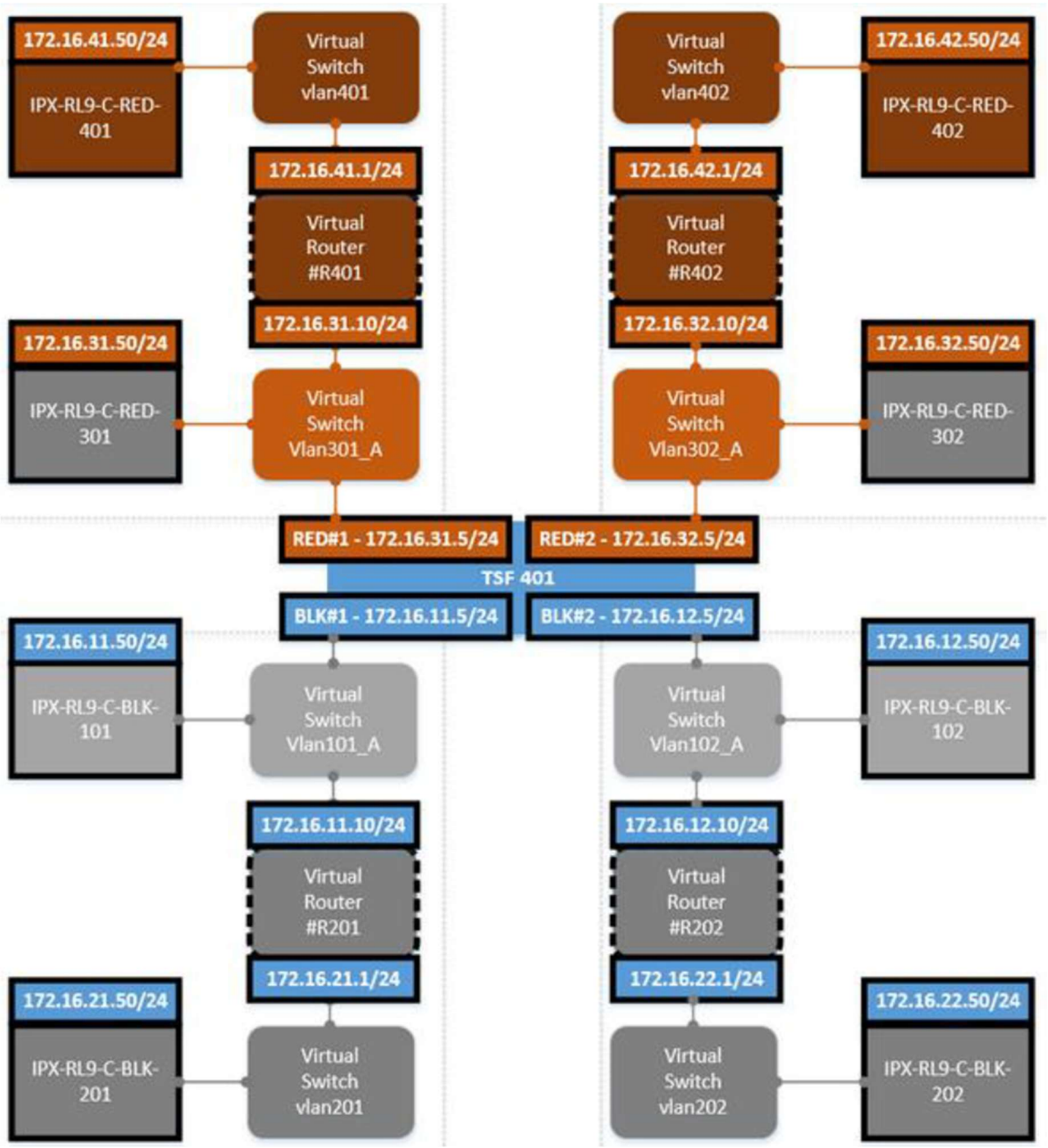

172.16.41.50/24
IPX-RL9-C-RED-401
Virtual Switch vlan401
172.16.41.1/24
Virtual Router #R401
172.16.31.10/24
172.16.31.50/24
IPX-RL9-C-RED-301
Virtual Switch Vlan301_A
Virtual Switch vlan402
172.16.42.50/24
IPX-RL9-C-RED-402
172.16.42.1/24
Virtual Router #R402
172.16.32.10/24
172.16.32.50/24
IPX-RL9-C-RED-302
Virtual Switch Vlan302_A
RED#1 - 172.16.31.5/24
RED#2 - 172.16.32.5/24
TSF 401
BLK#1 - 172.16.11.5/24
BLK#2 - 172.16.12.5/24
172.16.11.50/24
IPX-RL9-C-BLK-101
Virtual Switch Vlan101_A
172.16.11.10/24
Virtual Router #R201
172.16.21.1/24
172.16.21.50/24
IPX-RL9-C-BLK-201
Virtual Switch vlan201
Virtual Switch Vlan102_A
172.16.12.50/24
IPX-RL9-C-BLK-102
172.16.12.10/24
Virtual Router #R202
172.16.22.1/24
172.16.22.50/24
IPX-RL9-C-BLK-202
Virtual Switch vlan202

Figure 6

Figure 7 shows that in VLAN 101, several service functions have been established for testing purposes. This includes DHCP, NTP and SYSLOG servers. This setup allows for testing filter functions from the RED side to the BLACK side and back.

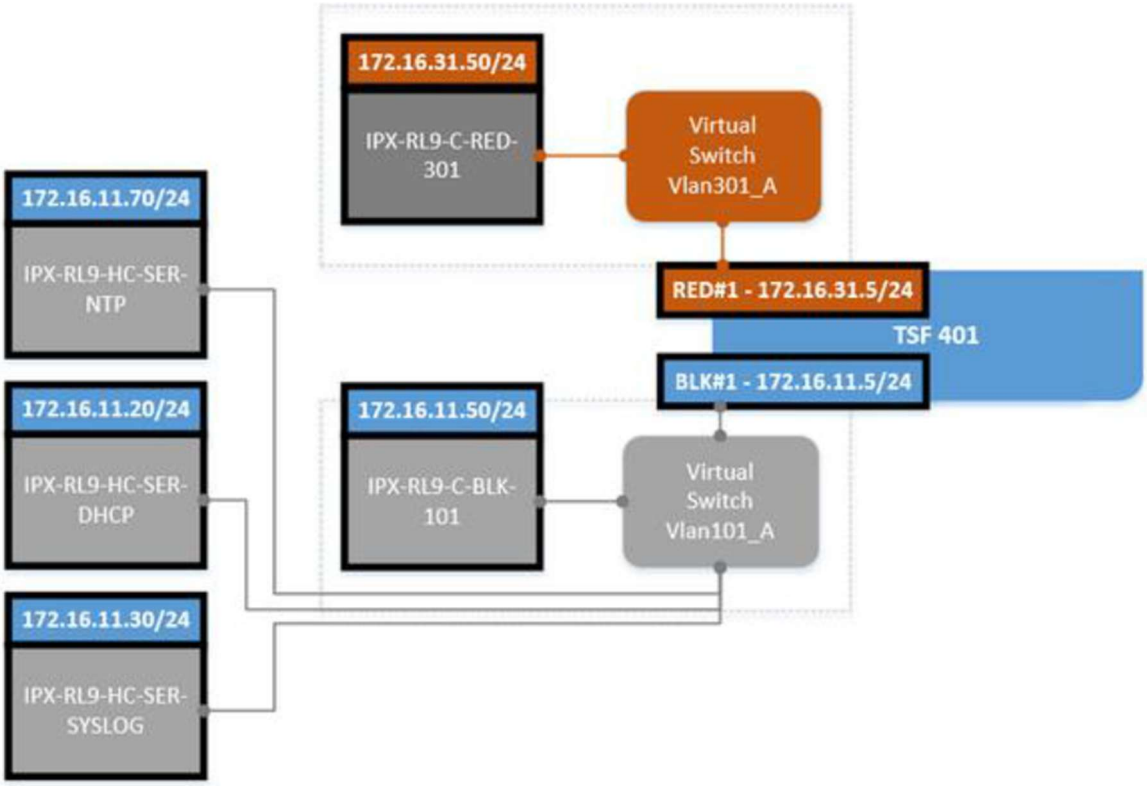


Figure 7

The configuration/testbed used for penetration testing of TOE:

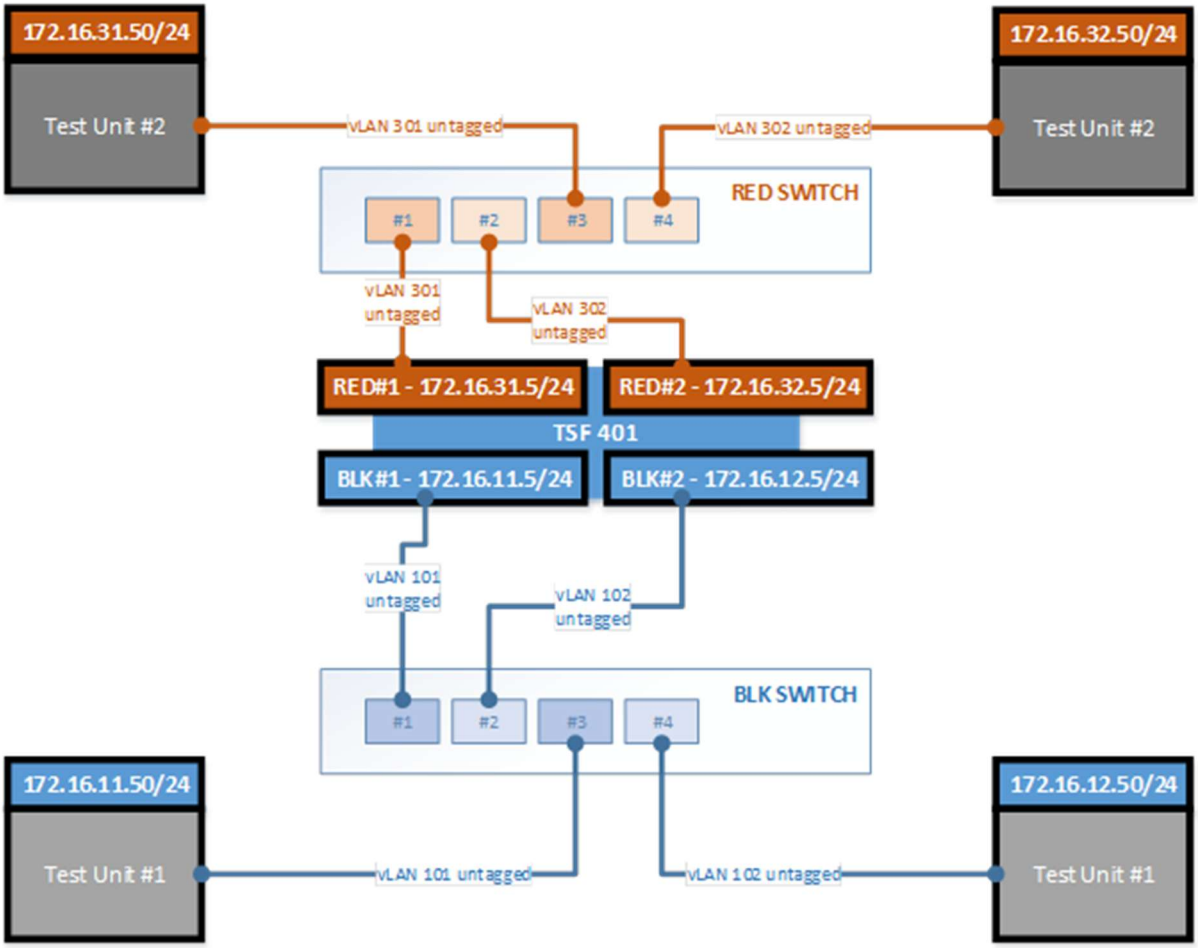


Figure 8