THALES

Trusted Security Filter
TSF 201

Security Target

THALES

DOCUMENT CHANGE HISTORY

Revision	Date	Description
001	23.06.2015	First approved version.
002	14.09.2015	Changed classification to “unclassified”.
003	02.11.2018	New version of TOE. New functionality: NAT, block traffic.
004	18.02.2020	New version of TOE. New functionality: Support for TCP traffic.

	–	001	002	003	004		
Written by	SE Team	**Kjell Kristiansen**	**Kjell Kristiansen**	**Kjell Kristiansen**	**Morten Olderkjær**		
Checked by	QA Manager	**Tore Grønvold**	**Tore Grønvold**	**Svein Ringstad**	**Svein Ringstad**		
Approved by	PDA	**Knut Lillegraven**	**Knut Lillegraven**	**Odd Arne Samdal**	**Odd Arne Samdal**		

THALES

Table of Contents

1. SECURITY TARGET INTRODUCTION (ASE_INT)

1.1 Security Target reference

(1) The following table identifies the Security Target (ST).

Item	Identification
ST title	Security Target for TSF 201
ST reference	3AQ 25940 AAAA 377 EN
ST version	See revision in footer
ST author	Thales Norway AS

1.2 Referenced documents

Id	Title
[1]	Lov om forebyggende sikkerhetstjeneste (SIKKERHETSLOVEN), av 20. mars 1998 nr. 10.

1.3 TOE reference

(1) The following table identifies the Target Of Evaluation (TOE)

Target of Evaluation (TOE) Identification	Trusted Security Filter (TSF 201); comprising: HW version: 3AQ 25960 BAAA rev. E SW version: 3AQ 25950 AAAA rev. 2.6
TOE Developer	Thales Norway AS

1.4 TOE overview

(1) The TOE is a contents-filtering gateway consisting of both hardware and software.

(2) It enables data transfer in a secure manner between two IP networks of different security classifications. Its design shall be trusted to perform separation of data between a HIGH (high security classification) network and a LOW (low security classification) network in a way upholding the security policy concerning data export and import between the individual networks.

(3) It is designed for use in a highly specialized IT environment.

(4) The TOE can be configured as a data diode that only allows data transfer from the LOW network to the HIGH network and blocks all data transfer in the other direction. Conversely, the TOE can be configured to block all data from the LOW network to the HIGH network.

(5) The TOE records auditable events in an audit log that is protected from change and deletion. It can be viewed by authorized users.

(6) The TOE has cryptographic functions to decrypt filter configuration files and software update files.

(7) The TOE has an emergency erase function to securely delete cryptographic keys and filter configuration files.

(8) The TOE has extensive self-test functions to support a fail secure design where single faults shall not violate the trusted functionality.

(9) The TOE has tampering detection and also passive protection in terms of tampering seals. The electronic tampering detection will trigger emergency erase.

(10) TSF 201 is TEMPEST certified. TEMPEST certification is outside the scope of the evaluation described in this document.

1.5 TOE description

1.5.1 General

(1) This section presents an overview of the TSF 201 (the TOE) and its environments.

1.5.2 TOE application

(1) Figure 1-1 shows a schematic example of how the TOE may be deployed in an IP based system.

(2) The purpose of the TOE is to operate as a data filter (firewall) between a HIGH network (e.g. a network classified HEMMELIG/NATO SECRET or equivalent) and a LOW network (e.g. an UGRADERT/UNCLASSIFIED network or a network classified BEGRENSET/NATO RESTRICTED or equivalent). Each of the two networks will consist of one or more end systems of different types. The end systems may be connected to the same subnets as the TOE, or they can be reached via a router connected to the same subnet as the TOE.

NOTE: The HIGH network can have a highest classification of HEMMELIG/NATO SECRET, but it can also be less. It will always be one or more classification levels above the LOW network.

(3) The TOE shall typically permit all UDP and TCP traffic from the low classification system to the high classification system, and permit filtered UDP and TCP traffic from the high classification system to the low classification system, while traffic using other transport protocols than UDP and

TCP will not be allowed to pass through the TOE. However, it is possible to block all traffic from the low classification to the high classification.

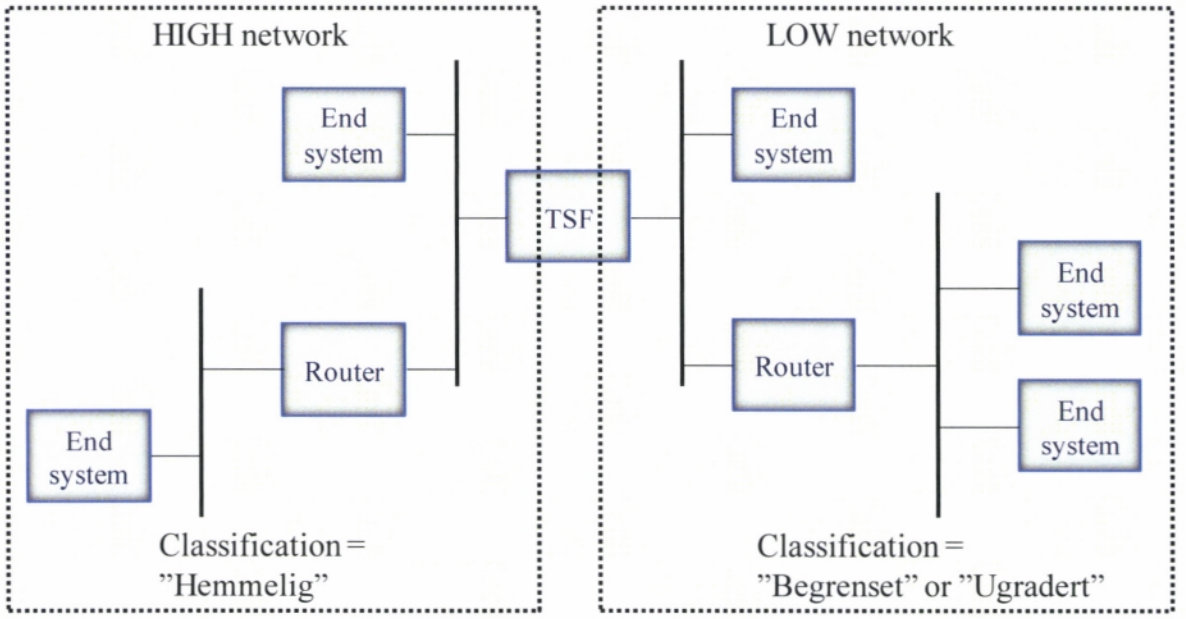

Figure 1-1 System example

(4) The TOE communication interfaces to the HIGH network and the LOW network are sometimes denoted 'red interface' and 'black interface' respectively, although no encryption of the data traffic through the TOE takes place. Similarly, the HIGH network and the LOW network are sometimes denoted 'red network' and 'black network'.

(5) The term TOE manager is used as general term for the two roles Security operator and Operator that are defined within the TOE management. The Security operator has access to all functions including importing of keys, software and new filter configuration files; the Operator has access to monitoring functions, configuration of Ethernet interfaces and selection of filter configuration files from the available choices.

(6) The TOE shall support up to 10 different filters. One of the filters is hardcoded in the TOE and will provide a diode function, allowing UDP and TCP traffic from the black network to the red network and no traffic from the red network to the black network. Up to 9 filters may be loaded from the Local Management interface. A filter is a configuration file specifying the content of the UDP and TCP messages that shall be allowed to pass from the red to the black network. To maintain integrity and confidentiality each file is encrypted and cryptographically signed during production and will be stored encrypted in the TOE. The TOE manager selects, during installation, the filter to be used in the actual network, prior to operational use. Moreover, it is possible to configure the TOE to block all traffic from the black to the red network, while maintaining a filter from the red to the black side.

(7) The TOE supports a default gateway on HIGH side and a default gateway on LOW side. This means that the communicating end systems must either be connected to the same Local Area Networks as the TOE, or can be reached via a router that must be configured as default gateway in the TOE.

(8) The TOE can be configured with NAT functionality that changes the source address in the IP packets routed from LOW to HIGH to the red IP address of the TOE.

1.5.3 System interfaces

(1) The TOE has 4 external interfaces for exchange of end user data or management data, shown in Figure 1-2

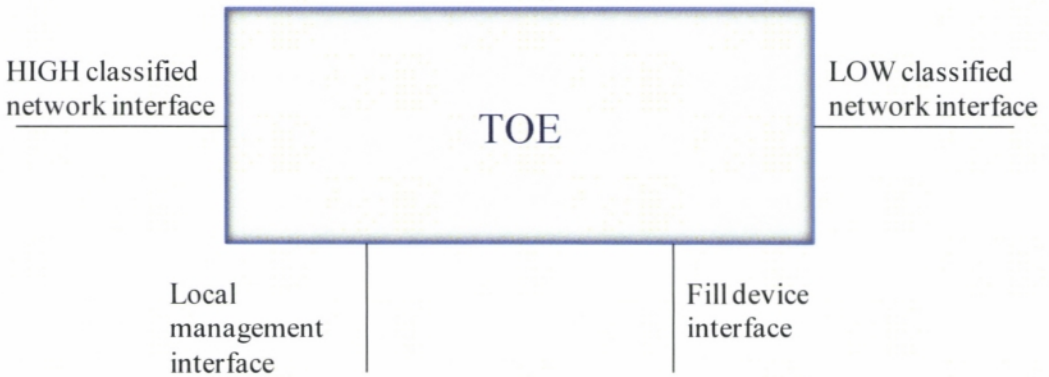

Figure 1-2 TOE external interfaces

(2) These interfaces are available on 4 different connectors.

(a) HIGH network interface:
This interface is an Ethernet interface used for connection to the HIGH network. A standard 100 Mbit/s interface is supported by means of a special cable, and a 100BASE-FX optical interface is supported by means of a special optical adapter developed by Thales Norway.

(b) LOW network interface:
This interface is an Ethernet interface for connection to the LOW network, with characteristics identical to the high classified network interface.

(c) Local Management interface:
The TOE operators are the authorized users that use this Ethernet interface for web based management of the TOE, and for loading of cryptographically signed filter configuration files or cryptographically signed SW update images for the TOE. The IP address of this interface is set to 192.168.0.1 and cannot be changed.

(d) Fill device interface:
This interface is an ISO-7816/3 interface for loading of cryptographic keys from smart card via an external Tempest approved smart card reader.

(3) In addition the TOE has the following external interfaces:

(a) CIK interface:
This interface is to support the use of a CIK plug-in unit.

(b) Light Emitting Diode (LED) indicators.

(c) Numeric keypad (optionally used if the TOE is configured to use PIN code).

(d) Power interface:
The power input is 10 – 60 V DC from a battery or an external power adapter.

1.5.4 The TOE components

1.5.4.1 General

(1) As Figure 1-3 shows, the TOE is divided into four separated nodes, two Service nodes interfacing one network each, a Filter node interfacing the Service nodes, and a Key Fill node interfacing the fill device interface.

(2) The nodes run on dedicated hardware; CPU, memory, FPGA, in order to achieve the necessary separation of domains.

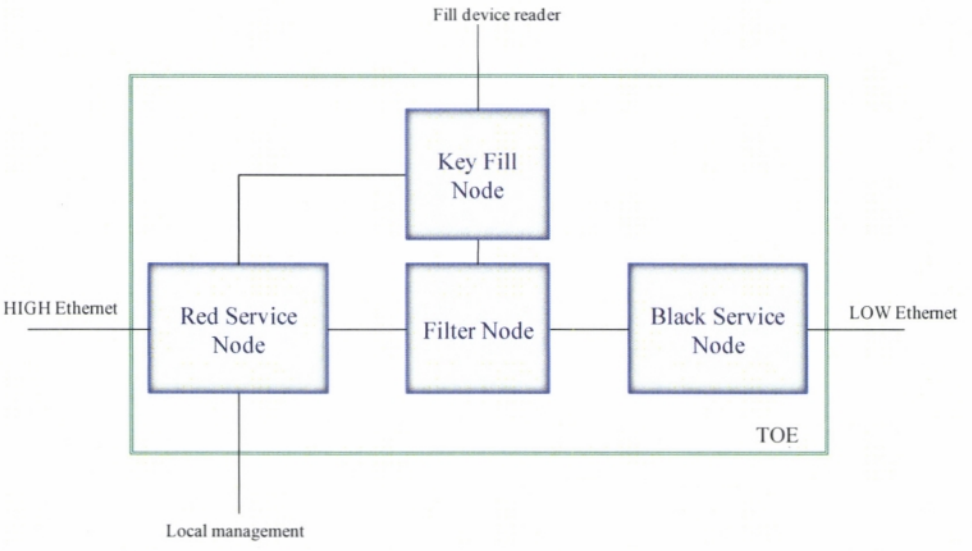

Figure 1-3 TOE Components

1.5.4.2 Service Nodes

(1) The service nodes receive data from the connected networks and perform initial filtering of unwanted protocols before presenting the data to the Filter Node. In addition, the Red Service Node has a web server for configuration and storage of local management data that can be accessed from a web client on a standard PC using SSL protocol.

1.5.4.3 Filter Node

(1) The Filter Node, depending on the configuration, will filter the traffic from red to black interface according to filter rules defined configuration files loaded from local management. These files are produced in an offline tool, then encrypted and signed before loaded into the TOE. The TOE will decrypt and verify the digital signature.

(2) The Filter Node always has a diode mode allowing traffic from black to red interface. The filter modes pertaining traffic in the other direction depends on whether filter configuration files has been loaded.

(3) The filter node has specific self-test functions to support a fail-secure design. Single failures shall not violate the trusted functionality.

(4) The filter node monitors the rate of flow of legal messages through the filter and generates audit events if the rate exceeds thresholds defined in the filter configuration files.

1.5.4.4 Key Fill Node

(1) The Key Fill Node has the interface to the smart card fill device used for loading of keys for the filter configuration files and SW update files.

1.5.5 TOE front panel

(1) Figure 1-4 shows the TOE front panel with the external connectors and local management facilities. In this figure, the terms 'Red communication interface' is the same as 'HIGH network interface', and 'Black communication interface' is the same as 'LOW network interface'.

(2) All connectors intended to be handled by installation and maintenance are located at the front. The front also has indicator lamps providing information of the status and alarms of the TOE.

(3) The power switch in Figure 1-4 has an emergency erase mode to securely delete cryptographic keys and filter configuration files.

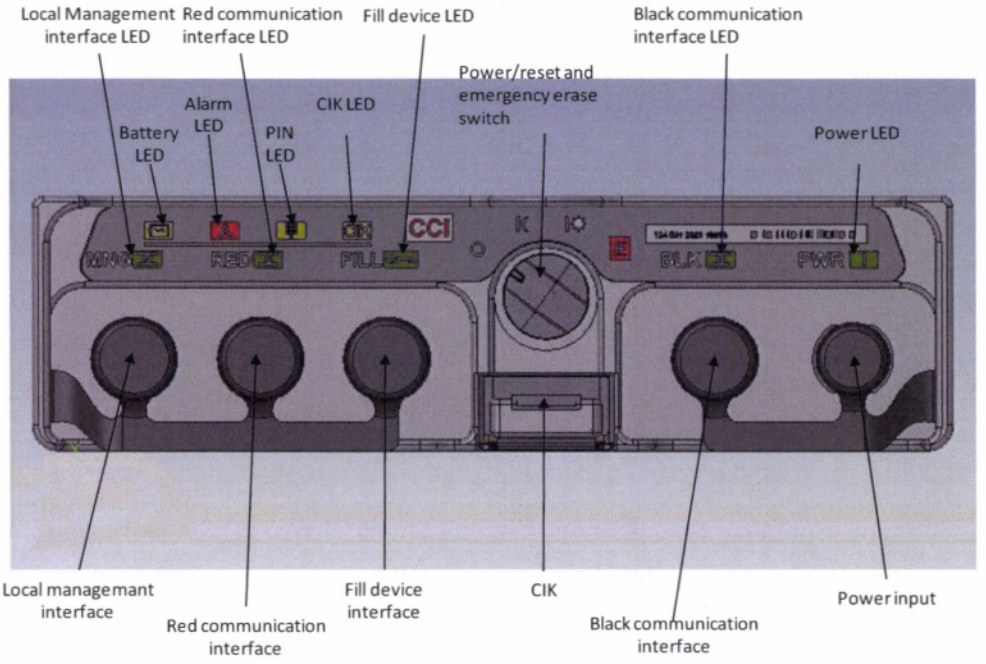

Figure 1-4 TOE communication and operator interfaces

1.6 Conventions

(1) The notation, formatting and conventions used in this Security Target are consistent with those used in version 3.1 of the Common Criteria (CC).

(2) The CC functional and assurance components may be used exactly as defined in CC Part 2 and CC Part 3, or they may be tailored through the use of permitted operations as described in CC Part 1, §8.1:

(3) The *assignment* operation occurs when a given component contains an element with a parameter that may be set by the Security Target author. The assignment is indicated by showing the value in square brackets with *italicized and underlined* text. Example:

(a) In CC Part 2 the component FAU_ARP.1.1 calls for an assignment:

(i) The TSF shall take [assignment: list of actions] upon detection of a potential security violation.

(b) The requirement is tailored by the assignment as follows:

(i) The TSF shall take [*an action to raise a local alarm*] upon detection of a potential security violation.

(4) The *selection* operation occurs where a given component contains an element where a choice from several items has to be made by the Security Target author. The selection is indicated by showing the value in square brackets with *italicized* text. Example:

(a) In CC Part 2, requirement FAU_STG.2.2 calls for a selection:

(i) The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

(b) The requirement is tailored by the selection as follows:

(i) The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in the audit trail.

(5) The *iteration* operation is used when there is more than one requirement based on the same component. Iteration is denoted by showing the iteration number in parenthesis following the component identifier. Example of how iterations can be used:

(a) If the Security Target should specify two requirements based on FAU_ARP.1 they would be denoted FAU_ARP.1(1) and FAU_ARP.1(2).

(6) The *refinement* operation is performed by altering the requirement. Refinements are indicated by **bold text** and ~~strikethrough~~.

(7) **Assumptions** are given names beginning with "A.".

(a) Example: A.PHYSICAL

(8) **Threat agents** are given names beginning with "TA.".

(a) Example: TA.INTERNAL

(9) **Threats** are given names beginning with "T.".

(a) Example: T.TAMPERING

(10) **Policies** statements are given names beginning with "P.". Policy statements are not used in this Security Target.

(11) **Security objectives** are given names as follows:

(a) IT Security Objectives applicable for the TOE are given names beginning with "O.".

(i) Example: O.AUDIT

(b) Non-IT Security Objectives applicable for the TOE are given names beginning with "NO.".

(i) Example: NO.SEALING

(c) IT Security Objectives applicable for the environment are given names beginning with "OE.".

(i) Example: OE.AUDIT

(d) Non-IT Security Objectives applicable for the environment are given names beginning with "NOE.".

(i) Example: NOE.INSTALL

2. CONFORMANCE CLAIMS (ASE_CCL)

2.1 CC conformance claim

Conformance	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002 Part 3: Security Assurance Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003
Assurance level	EAL5 augmented with ALC_FLR.3 (Systematic flaw remediation)

2.2 PP and Package conformance claims

(1) The Security Target has no Protection Profile claims.

(2) The Security Target has no Package conformance claims.

3. SECURITY PROBLEM DEFINITION (ASE_SPD)

3.1 General

(1) This section provides the statement of the Security Problem Definitions, which identifies and explains all:

(a) Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

(b) Known and presumed threats countered by either the TOE or by the security environment.

(c) Organisational security policies the TOE must comply with.

3.2 Assumptions

(1) The following conditions are assumed to exist in the operational environment.

A.PHYSICAL	The system comprising the TOE and the HIGH network is installed in a physical protected area, minimum approved for information classified HIGH. This applies also to the local management and the channel from the local management. The LOW network is installed in a physical area minimum approved for protection of the information classified LOW.
A.TRAINING	All TOE managers are trained in the correct use of the TOE.
A.CLEARANCE	All TOE managers have a minimum clearance for the security level HIGH, and is authorised for all information handled by the system.
A.MAN.AUTHORISED	Only managers with special authorisation are allowed to do configuration and management of the system including TOE.
A.USAGE	The TOE is used between two LANs in a protected environment and is installed according to the installation guidelines for the TOE.

3.3 Threats

3.3.1 General

(1) This section identifies the assets, threat agents and threats.

3.3.2 Identification of assets

(1) The assets that TOE shall protect as specified in this Security Target are the following:

(a) Information with HIGH security classification,

(b) Cryptographic keys,

(c) Filter configuration files.

(2) In addition the TOE shall provide TEMPEST protection of both HIGH and LOW information, but this is outside the scope of this CC evaluation.

3.3.3 Identification of threat agents

TA.INTERNAL	Personnel that have authorised access to the installations of the TOE and/or the HIGH network and which has intent to perform unauthorised actions. These persons may be trained specially to perform their unauthorised actions. They may bring unauthorised software into the site and may be able to load it. They may be supported by entities with unlimited resources.
TA.EXTERNAL	Personnel that do not have access to the installations of the TOE and/or the HIGH network and which has the intent to divulge classified information, in particular information with HIGH security classification. These persons may have unlimited resources.
TA.USER	Users with no intent to perform unauthorised actions. They may unintentionally perform unauthorised actions.
TA.TECHNICIAN	Technicians with no intent to perform unauthorised actions. They may unintentionally perform unauthorised actions.
TA.MALFUNCTIONS	System malfunctions. System malfunctions to be considered are limited to single point of failure.

3.3.4 Threats

T.CONN.HIGH.LOW	Information with HIGH security classification on the HIGH network may be transferred to the LOW network.
Threat agents	TA.TECHNICIAN, and/or TA.MALFUNCTIONS. In addition the following must be present: TA.EXTERNAL
Asset	Information classified HIGH.
Unwanted outcome	Unauthorised personnel get access to information classified HIGH.

Attack methods	A technician (TA.TECHNICIAN) unintentionally configures or installs the TOE in a way that transfers information with HIGH security classification on the HIGH network to the LOW network. The HIGH information is picked up from the LOW network by persons (TA.EXTERNAL) outside the physically protected area for HIGH information. A malfunction in the TOE implies that HIGH information on HIGH network is transferred to the LOW network. The HIGH information is picked up from the LOW network by persons (TA.EXTERNAL) outside the physically protected area for HIGH information
T.TAMPERING	Security-critical part of the TOE may be subject to physical attack that may compromise security.
Threat agents	TA.INTERNAL combined with TA.EXTERNAL
Asset	Information classified HIGH.
Unwanted outcome	Unauthorised personnel get access to information classified HIGH.
Attack method	A person (TA.INTERNAL) modifies the TOE to transfer HIGH information from the HIGH network to the LOW network. The classified information is picked up from the LOW network by persons (TA.EXTERNAL) outside the physically protected area for HIGH information.
T.MISUSE	An attacker may transfer information classified HIGH from the HIGH network to the LOW network, by the use of data messages.
Threat agents	TA.INTERNAL combined with TA.EXTERNAL
Asset	Information classified HIGH.
Unwanted outcome	Unauthorised personnel get access to information classified HIGH.
Attack method	A person (TA.INTERNAL) introduce/modify software and/or hardware in the HIGH network to pick up information classified HIGH and transfer this information to the LOW network via the TOE. The information classified HIGH is picked up from the LOW network by persons (TA.EXTERNAL) outside the physically protected area for HIGH information. This threat increases if this can continue undetected.
T.TEMPEST	Electromagnetic emanations may divulge classified information.
Threat agents	TA.EXTERNAL possibly in combination with TA.INTERNAL
Asset	Information classified HIGH or LOW.
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	Information on the HIGH network or the LOW network is electromagnetically emanated to where it can be intercepted.

T.UNAUTHORISED.USE	Authorised persons on the HIGH system may perform unauthorised use of the HIGH system's applications and management system.
Threat agents	TA.INTERNAL or TA.USER. In addition the following must be present TA.EXTERNAL.
Asset	Information classified HIGH.
Unwanted outcome	Unauthorised personnel get access to information classified HIGH.
Attack method	Authorised persons may perform intentionally (TA.INTERNAL) or unintentionally (TA.USER) unauthorised use of the HIGH system's applications and management. The threat is that this may lead to transfer of information classified HIGH onto the LOW network. The HIGH information is picked up from the LOW network by persons (TA.EXTERNAL) outside the physically protected area for HIGH information.
T.ILLEGAL.CONFIG	An attacker attempts to: Modify or destroy authorised filter configuration files Modify or destroy keys used for decryption of filter configuration files Inject unauthorised filter configuration files Inject malicious code Into the TOE by unauthorised access through the administration interface.
Threat agents	TA.INTERNAL combined with TA.EXTERNAL
Asset	Information classified HIGH. Cryptographic keys and filter configuration files.
Unwanted outcome	Unauthorised personnel get access to information classified HIGH or unauthorised personnel succeeds in a denial of service.
Attack method	A person (TA.INTERNAL) is able to manipulate the filter configuration file or TOE SW image and introduce/modify the software in the TOE through the local management interface with the intent to transfer information classified HIGH to the LOW network. The HIGH information is picked up from the LOW network by persons (TA.EXTERNAL) outside the physically protected area for HIGH information.
T.SECURE.KEY	An attacker attempts to: Obtain the cryptographic keys for the purpose of decrypting and modifying the filter configuration files.
Threat agents	TA.INTERNAL combined with TA.EXTERNAL
Asset	Information classified HIGH. Cryptographic keys and filter configuration files.
Unwanted outcome	Unauthorised personnel get access to information classified HIGH.
Attack method	A person (TA.INTERNAL or TA.EXTERNAL) is able to obtain the cryptographic keys and a filter configuration file, and is able to manipulate and encrypt a filter configuration file in such a way that HIGH data is transmitted to the LOW network. The HIGH information is picked up from the LOW network by persons (TA.EXTERNAL) outside the physically protected area for HIGH information.

3.4 Organisational security policies

Not applicable.

4. SECURITY OBJECTIVES (ASE_OBJ)

4.1 TOE IT security objectives

O.ALARM.FAILURE	If a hardware or software failure is detected in the TOE, the TOE shall raise a local alarm.
O.AUDIT	The TOE shall have a protected audit log (residing in permanent memory and not possible to delete by the user) that can be viewed by a web browser on the HIGH network.
O.CRYPTO	The TOE shall have cryptographic functions to decrypt filter configuration files and software update files and for encryption of internal keys.
O.FW.THRESHOLD	The TOE shall perform flow monitoring of messages handled by the filter and shall generate an audit event if the threshold of legitimate messages is exceeded.
O.FILTER	Information classified HIGH shall be prevented from being transmitted to the LOW network.
O.KEY.GENERATE	The TOE shall have a mechanism to generate cryptographic keys that are for internal use only.
O.KEY.LOAD	The TOE shall have a mechanism to load cryptographic keys. The keys shall be integrity protected.
O.NO.CONFIG	The firewall filter shall not be configurable inside the TOE. The TOE manager shall be able to select sets of predefined filter criteria.
O.ROBUST.TOE.ACCESS	The TOE shall provide mechanisms that control the administrator's logical access to the TOE local management interface and to explicitly deny access to non-authorised users. The TOE shall provide two operator roles (users): • Operator • Security operator (access to both operator and security operator functions) Authentication of users shall be based on pin code (optional), operator role and password.
O.SECURE.CHANNEL	The TOE shall use asymmetric encryption techniques to establish a secure channel between the TOE and a web client presenting the local management information.
O.SECURE.CONFIGURATION	TOE filter files and software update files can be loaded from the local management interface. Filter configuration files and software are protected by encryption and digital signature. Prior to accepting a new file, the TOE shall perform the following verification: • The file shall be decrypted, • The integrity and authenticity shall be verified by means of a digital signature

	• Known Answer Tests shall be run (filters only), If the decryption and verification of signature fails or Known Answer Test fails, the update shall be rejected.
O.SELF.TEST	Security critical functions shall be tested by a combination of power-up tests, periodic tests and continuous tests.
O.EMERGENCY.ERASE	The TOE shall provide automatic and manual functions for emergency erase of cryptographic keys and filter configuration files. The emergency erase shall be triggered automatically upon tamper detection or be manually initiated from the front panel.

4.2 TOE Non-IT security objectives

NO.SEALING	The TOE shall be sealed in such a way that it is easy to see that it has been opened/tampered with.
NO.TEMPEST	TEMPEST evaluation and certification of the TOE is performed by NSM. This certification ensures that NO.TEMPEST is achieved. This aspect is not treated further in this document.

4.3 Environment IT security objectives

OE.AUDIT	The IT environment shall be able to display the web page with the audit log. The web server resides in the TOE and the audit log is protected by the TOE
OE.KEY.GENERATE	The IT environment shall be able to generate cryptographic keys that the TOE uses to decrypt filter configuration files and software update files. The cryptographic keys shall be administered according to: [1] - Forskrift om informasjonsikkerhet – kapittel 7 Administrativ kryptosikkerhet.
OE.MAN.ACCESS	Special authorisation is required to grant access to configure and manage the TOE.

4.4 Environment non-IT security objectives

NOE.ACCESS.CTRL	Only authorised persons shall be given physical access to the system comprising the TOE and the HIGH network.
NOE.AUDIT	Authorised managers of the TOE must ensure that the TOE audit log are used and managed effectively. On particular, TOE 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.
NOE.CI	The TOE shall be treated as CI material according to: [1] - Forskrift om informasjonsikkerhet – kapittel 7 Administrativ kryptosikkerhet.
NOE.CLEARANCE	All users shall have a minimum clearance for the maximum-security level of information handled in the system.
NOE.INSTALL	The responsible for the TOE must ensure that the TOE is installed according to the installation guidelines for the TOE.
NOE.KEY.DESTRUCT	The cryptographic keys shall be destructed according to: [1] - Forskrift om informasjonsikkerhet – kapittel 7 Administrativ kryptosikkerhet.
NOE.MAN.TRAIN	The TOE managers are fully trained to use and interpret the TOE equipment.
NOE.PHYS. PROT	The site where the TOE is installed shall have physical protection. The level of protection shall be approved for minimum security level HIGH.

4.5 Security objectives for the TOE rationale

Threats/ Assumptions / Objectives	T.CONN.HIGH.LOW	T.TAMPERING	T.MISUSE	T.TEMPEST	T.UNAUTHORISED.USE	T.ILLEGAL.CONFIG	T.SECURE.KEY	A.PHYSICAL	A.TRAINING	A.CLEARANCE	A.MAN.AUTHORISED	A.USAGE
O.ALARM.FAILURE	x											
O.AUDIT			x									
O.CRYPTO			x			x						
O.FW.THRESHOLD			x									
O.FILTER	x		x									
O.KEY.GENERATE							x					
O.KEY.LOAD							x					
O.SELF.TEST	x											
O.NO.CONFIG	x				x							
O.ROBUST.TOE.ACCESS						x	x					
O.SECURE.CONFIGURATION						x						
O.EMERGENCY.ERASE		x					x					
O.SECURE.CHANNEL					x							
NO.SEALING		x										
NO.TEMPEST	x			x								
OE.AUDIT			x									
OE.KEY.GENERATE							x					
OE.MAN.ACCES					x						x	
NOE.ACCESS.CTRL								x		x		
NOE.AUDIT			x									
NOE.CI		x					x		x			
NOE.CLEARANCE										x		

NOE.INSTALL	x			x				x	x			x
NOE.MAN.TRAIN	x		x						x			
NOE.PHYS.PROT		x						x				

Table 1 Mapping of Objectives to Threats and Assumptions

4.5.1 General

(1) As can be seen fromTable 1, at least one objective, either TOE or environment, as applicable meets all threats and assumptions. The coverage of the threats and assumptions countered by the TOE is discussed in the subsections below.

4.5.2 T.CONN.HIGH.LOW

(1) The TOE controls the separation of LOW and HIGH information and the information flowing from the HIGH to the LOW network (O.FILTER) which is not configurable (O.NO.CONFIG). A failure in domain separation will be detected during power-up and/or normal operation (O.SELF.TEST). A local alarm indication is given by detection of hardware or software failure (O.ALARM.FAILURE). The TOE managers are fully trained to handle and interpret the TOE equipment (NOE.MAN.TRAIN). The TOE is installed (NOE.INSTALL) and given TEMPEST protection (NO.TEMPEST) according to established guidelines.

4.5.3 T.TAMPERING

(1) To prevent tampering the TOE is installed in physical protected area that is provided with access control system (NOE.PHYS.PROT). The TOE is also sealed, so it is easy to see that the seal has been broken (NO.SEALING). Periodical manual inspection will detect possible tampering (NOE.CI). The TOE has a tampering detection for erasing cryptographic keys and filter configuration files (O.EMERGENCY.ERASE)

4.5.4 T.MISUSE

(1) Filter configuration files are protected until they are activated within the TOE (O.CRYPTO). All messages from the HIGH network to the LOW network are checked in the TOE firewall (O.FILTER). The TOE will count all messages that are allowed to pass the firewall and generate an audit event if the count for a message exceeds the threshold (O.FW.THRESHOLD). The TOE will store event on rejected messages in the audit log (O.AUDIT). The TOE manager is trained (NOE.MAN.TRAIN) to inspect the firewall statistics and audit log (NOE.AUDIT) by means of a web browser (OE.AUDIT) to stop any attempt to misuse the covert channels.

4.5.5 T.TEMPEST

(1) The TOE shall be installed according to installation guidelines (NOE.INSTALL), which complies with the TEMPEST installation guidelines (NO.TEMPEST).

4.5.6 T.UNAUTHORISED.USE

(1) The web client used for local management must have a certificate issued by the TOE and use asymmetric techniques for establishing a secure communication channel with the TOE (O.SECURE.CHANNEL). TOE operators need special authorisation to handle the configuration and management part of the TOE (OE.MAN.ACCES). A filter is not configurable from TOE management (O.NO.CONFIG).

4.5.7 T.ILLEGAL.CONFIG

(1) TOE managers must be authenticated to gain access to the TOE local management and only the role Security operator is allowed to import data (O.ROBUST.TOE.ACCESS). The TOE filter configuration files and software update files are protected against manipulation both during transportation to the TOE and within the TOE (O.CRYPTO). The filter configuration files must be authenticated when loaded into the TOE and before activation (O.SECURE.CONFIGURATION).

4.5.8 T.SECURE.KEY

(1) The TOE has a mechanism for loading of cryptographic keys (O.KEY.LOAD). TOE managers must be authenticated and only the role Security operator is allowed to load cryptographic keys (O.ROBUST.TOE.ACCESS). Cryptographic keys are erased upon tamper detection (O.EMERGENCY.ERASE). Cryptographic keys are generated (OE.KEY.GENERATE) and administered according to established rules (NOE.CI). TOE generates cryptographic keys for internal use only (O.KEY.GENERATE).

4.5.9 A.PHYSICAL

(1) The TOE must be installed according to the installation guidelines (NOE.INSTALL). Only authorised persons shall be given physical access to the system comprising the TOE and the connected networks (NOE.ACCESS.CTRL). The TOE must be installed in a physical protected area, minimum approved for the highest security level of information handled in the system (NOE.PHYS.PROT).

4.5.10 A.TRAINING

(1) The TOE managers are fully trained to handle and interpret the TOE (NOE.CI and NOE.MAN.TRAIN). The technicians should be trained to install the TOE according to the installation guidelines (NOE.INSTALL).

4.5.11 A.CLEARANCE

(1) Only authorised persons shall be given physical access to the system comprising the TOE and the connected networks (NOE.ACCESS.CTRL and NOE.CLEARANCE).

4.5.12 A.MAN.AUTHORISED

(1) Special authorisation is required to grant access to handle configuration and management of the TOE (OE.MAN.ACCESS).

4.5.13 A.USAGE

(1) The TOE must be installed according to the installation guidelines (NOE.INSTALL).

5. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

(1) The following explicit components have been included in this Security Target because the Common Criteria components were found to be insufficient as stated.

5.1 Explicit Functional Components

Explicit Component	Identifier	Rationale
FPT_DES_EXT.1	Destruction of filter configuration files	This explicit component is necessary since it describes the destruction of filter configuration files

6. SECURITY REQUIREMENTS

6.1 General

(1) This section contains the functional requirements that are provided by the TOE and the IT environment. These requirements consist of functional components from Part 2 of the Common Criteria (CC), extended with explicitly stated requirements.

6.2 TOE Security Functional Requirements

(1) The Table 2 list the functional components included in this ST.

Functional class	Component	Name
FAU – Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Security audit review
	FAU_STG.1	Protected audit trail storage
FCS – Cryptographic Support	FCS_COP.1(1)	Cryptographic operation (filter configuration and SW update files)
	FCS_COP.1(2)	Cryptographic operation (local management communication)
	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
FDP – User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Access control functions
	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
	FDP_IFF.6	Illicit information flow monitoring
	FDP_ITC.2	Import from outside of the TOE
FIA – Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	User authentication
	FIA_UID.2	User identification
FMT – Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_SMF.1	Specification of Management Functions

	FMT_SMR.1	Security roles
FPT – Protection of the TSF	FPT_DES_EXT.1	Destruction of filter configuration files
	FPT_FLS.1	Failure with preservation of secure state
	FPT_PHP.1	Passive detection of physical attack
	FPT_STM.1	Reliable Time Stamps
	FPT_TDC.1	Inter-TSF basic TSF data consistency
	FPT_TST.1	TSF self test
FTP – Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel

Table 2 TOE Security Functional Requirements

6.2.2 Security Functional Policies

(1) The following information flow control policies are being used:

6.2.2.2 Traffic_Data Information Flow Control Policy

(1) The Traffic_Data information flow control policy regulates how the TOE shall maintain the network separation security policy. The SFP is defined by FDP_IFC.2 and FDP_IFF.1 The Traffic_Data information flow control policy is monitored for illicit information defined by FDP_IFF.6.

6.2.2.3 Configuration Access Control Policy

(1) The Configuration access control policy regulates the access to Security Configuration including authentication of the role Security operator at login. The SFP as defined by FDP_ACC.1 and FDP_ACF.1. The Configuration access control policy is referenced in FDP_ITC.2, ensuring a secure import of filter configuration files and software update files, and also ensuring a secure loading of cryptographic keys trough a dedicated interface and trusted channel FTP_ITC.1.

6.2.3 Security audit

(1) This section involves recognising, recording and storing information related to security relevant activities.

FAU_ARP.1	Security alarms
FAU_ARP.1.1	The TSF shall take [*an action to raise a local alarm*] upon detection of a potential security violation.
	Dependencies: FAU_SAA.1 Potential violation analysis is included.

FAU_GEN.1	Audit data generation
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: Start-up and shutdown of the audit functions All auditable events for the [*not specified*] level of audit; and [*Exceeding threshold values*].
	Dependencies: FPT_STM.1 Reliable time stamps is included.
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*].

FAU_SAA.1	Potential violation analysis
FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: • Accumulation or combination of [*tampering protection, emergency erase, self tests*] known to indicate a potential security violation. • [*none*]
	Dependencies: FAU_GEN.1 Audit data generation is included.

FAU_SAR.1	Security audit review
FAU_SAR.1.1	The TSF shall provide [*TOE Manager*] with the capability to read [*all*] from the audit records.
FAU_SAR.1.2	The TOE SF shall provide the audit records in a manner suitable for the user to interpret the information.
	Dependencies: FAU_GEN.1 Audit data generation is included.

FAU_STG.1	Protected audit trail storage
FAU_STG.1.1	The TSF shall protect the stored audit records from unauthorised deletion.

FAU_ STG.1.2	The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in audit trail.
	Dependencies: FAU_GEN.1 Audit data generation is included.

6.2.4 Cryptographic support

(1) This section specifies the Cryptographic Support security requirements for the TOE.

FCS_COP.1(1)	Cryptographic operation (Filter configuration files and software update files)
FCS_COP.1.1	The TSF shall perform [*decryption and strong integrity verification of imported filter configuration files and imported SW update images, strong integrity verification of imported keys, encryption of internal keys] in accordance with a specified cryptographic algorithm [AES-256] and cryptographic key sizes [key size 256] that meet the following: [NIST Special Publication 800-38A, NIST Special Publication 800-38B, and FIPS Publication 197 Advanced Encryption Standard (AES)*].
	Dependencies: FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(2)	Cryptographic operation (local management communication)
FCS_COP.1.1	The TSF shall perform [HTTPS communication for local management with *Transport Layer Security 1.2 (TLS)] in accordance with a specified cryptographic algorithm [RFC 5246] and cryptographic key sizes [RFC 5246] that meet the following: [RFC 5246*].
	Dependencies: FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1	Cryptographic key generation
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*random generator*] and specified cryptographic key sizes [key size *256*] that meet the following: [*FIPS Publication 197 Advanced Encryption Standard (AES)*].
	Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.4	Cryptographic key destruction

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroisation*] that meets the following: [*NSM guidelines*].
	Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

6.2.5 User data protection

(1) This section specifies the User Data Protection security requirements for the TOE.

FDP_ACC.1	Subset access control
FDP_ACC.1.1	The TSF shall enforce the [*Configuration access control policy*] on [*TOE managers injecting Security configuration files and modifying and querying Dynamic Parameters*[1]]
	Dependencies: FDP_ACF.1 Access control functions,

FDP_ACF.1	Access control functions
FDP_ACF.1.1	The TSF shall enforce the [*Configuration access control policy*] to objects based on the following: [*Subjects and attribute: TOE Manager role (Security Operator, Operator), Password. Objects and attributes: Filter configuration file/software update file – Cryptographic checksum. Dynamic parameters – Initial values (factory settings), local management interface*]
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*Only Security Operator shall be authorised to inject filter configuration files and software update files. Security operator/Operator can change dynamic parameters. Prior to accepting the filter configuration files or software update files the following verification shall be done: Integrity and authenticity shall be verified by means of a cryptographic checksum*]

[1] IP addresses of TOE interfaces and NTP server.

FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*At first start-up after delivery or after emergency erase it shall be possible to perform pairing of TOE and local management PC based on digital certificates.*]
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*The TOE shall deny injection of filter configuration files or software update files from all interfaces other than the local management interface. The TOE shall deny injection of keys from all other interfaces other than the key fill interface.*]
	Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_IFC.2	Complete information flow control
FDP_IFC.2.1	The TSF shall enforce the [*information flow control SFP*] on [*the following subjects:* • *TOE HIGH domain functions and* • *TOE LOW domain functions* *for the following information:* • *potentially classified information (HIGH information) and* • *unclassified information (LOW information)*] and all operations that cause that information to flow to and from subjects covered by the SFP. Note: The TOE information flow control SFP includes the policy statement to reject unacceptable messages attempted transmitted from the HIGH domain to the LOW domain and allow information from the LOW domain to the HIGH domain.
FDP_IFC.2.2	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.
	Dependencies: FDP_IFF.1 Simple security attributes is included.

FDP_IFF.1	Simple security attributes
FDP_IFF.1.1	The TSF shall enforce the [*information flow control SFP*] based on the following types of subject and information security attributes: [*The subjects are identified as blocks in the information flow block diagram, which is a part of the Information flow control SFP. The Information flow shall be controlled by the Information flow control SFP*].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*The rules are specified in the information flow control SFP*].
FDP_IFF.1.3	The TSF shall enforce [*no additional information flow control SFP rules*].

FDP_IFF.1.4	The TSF shall explicitly authorize an information flow based on the following rules: [*stated in the information flow control SFP*].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [*none*].
	Dependencies: FDP_IFC.1 is covered as FDP_IFC.2 is included. FMT_MSA.3 is included.

FDP_IFF.6	**Illicit information flow monitoring**
FDP_IFF.6.1	The TSF shall enforce the [*Information flow control SFP*] to monitor the [*illicit information flows through the firewall*] when it exceeds the [*none*].
	Dependencies: FDP_IFC.1 Subset information flow control is covered as FDP_IFC.2 is included.

FDP_ITC.2	**Import from outside of the TOE**
FDP_ITC.2.1	The TSF shall enforce the [*Configuration access control policy*] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE [*none*]
	Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency

6.2.6 Identification and authentication

(1) This section specifies the Identification and Authentication of users of the TOE.

FIA_ATD.1	**User attribute definition**
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [*Role, password*].
	Dependencies: No dependencies

FIA_UAU.1	**User authentication**
FIA_UAU.1.1	The TSF shall allow [*user identification*] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
	Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2	**User identification before any action**
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
	Dependencies: No dependencies

6.2.7 Security management

(1) This section specifies the Security Management of the TOE.

FMT_MSA.1	Management of security attributes
FMT_MSA.1.1	The TSF shall enforce the [*Information flow control SFP*] to restrict the ability to [*modify*] the security attributes [*none*] to [*none*].
	Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control. FDP_IFC.1 Subset information flow control is covered as FDP_IFC.2 is included.] FMT_SMR.1 Security roles is included FMT_SMF.1 Specification of Management Functions is included

FMT_MSA.3	Static attribute initialization
FMT_MSA.3.1	The TSF shall enforce the [*Information flow control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the *SFP*.
FMT_MSA.3.2	The TSF shall allow the [*none*] to specify alternative initial values to override the default values when an object or information is created.
	Dependencies: FMT_MSA.1 Management of security attributes is included. FMT_SMR.1 Security roles is included.

FMT_SMF.1	Specification of management functions

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [*Selecting diode operation, inject filter, selecting sets of filter criteria that has been loaded from the local management interface*].
	Dependencies: No dependencies.

FMT_SMR.1	Security roles
FMT_SMR.1.1	The TSF shall maintain the roles [*Operator, Security operator*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
	Dependencies: FIA_UID.1 Timing of identification is included.

6.2.8 Protection of the TOE Security Functions

(1) This section specifies the Protection of the TSF of the TOE.

FPT_DES_EXT.1	Destruction of filter configuration files
	The TSF shall destroy filter configuration files in accordance with a specified destruction method [zeroisation] that meets the following: [NSM guidelines].
	Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security]

FPT_FLS.1	Failure with preservation of secure state
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: [*Critical errors in one of the nodes*].
	Dependencies: No dependencies.

FPT_PHP.1	Passive detection of physical attack
FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
	Dependencies: No dependencies.

FPT_STM.1	Reliable time stamps
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.

	Dependencies: No dependencies.

FPT_TDC.1	Inter-TSF basic TSF data consistency
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret [*the Security configuration files*] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use [*the following rules:* *Security_configuration file definition,* *Filter rules for traffic data contained in the security_configuration file,* *TOE_software update files*] when interpreting the TSF data from another trusted IT product.
	Dependencies: No dependencies.

FPT_TST.1	TSF self test
FPT_TST.1.1	The TSF shall run a suite of self tests [*during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*[*none*]] to demonstrate the correct operation of [*the TSF*].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of [*TSF data*].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of [*TSF*].
	Dependencies: No dependencies.

6.2.9 Trusted path/channels

(1) This section specifies the trusted path/channels of the TOE.

FTP_ITC.1	Inter-TSF trusted channel
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [*loading of cryptographic keys*].
	Dependencies: No dependencies.

6.3 TOE security assurance requirements

(1) The assurance level of the TOE is EAL5 augmented with ALC_FLR.3 Systematic flaw remediation. The assurance components are summarised in Table 3 below.

Assurance class	Assurance component name	Assurance family
ADV: Development	Security Architecture description	ADV_ARC.1
	Complete semi-formal functional specification with additional error information	ADV_FSP.5
	Implementation representation of the TSF	ADV_IMP.1
	Well-structured internals	ADV_INT.2
	Semi-formal modular design	ADV_TDS.4
AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
ALC: Life Cycle Support	Production support, acceptance procedures and automation	ALC_CMC.4
	Development tools CM coverage	ALC_CMS.5
	Delivery procedures	ALC_DEL.1
	Identification of security measures	ALC_DVS.1
	Systematic flaw remediation	ALC_FLR.3
	Developer defined life-cycle model	ALC_LCD.1
	Compliance with implementation standards	ALC_TAT.2
ASE: Security Target Evaluation	Conformance claims	ASE_CCL.1
	Extended components definition	ASE_ECD.1
	ST introduction	ASE_INT.1
	Security objectives	ASE_OBJ.2
	Derived security requirements	ASE_REQ.2
	Security problem definition	ASE_SPD.1
	TOE summary specification	ASE_TSS.1
Class ATE: Tests	Analysis of coverage	ATE_COV.2
	Testing: modular design	ATE_DPT.3
	Functional testing	ATE_FUN.1
	Independent testing – sample	ATE_IND.2
AVA: Vulnerability assessment	Methodical vulnerability analysis	AVA_VAN.4

Table 3 Security assurance requirements: EAL5

6.4 Security requirements rationale

6.4.1 Requirements are appropriate

Table 4 identifies which SFRs satisfy the Objectives in chapter 4.

Component / Objectives	FAU_ARP.1	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_COP.1(1)	FCS_COP.1(2)	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FDP_IFF.6	FDP_ITC.2	FIA_ATD.1	FIA_UAU.1	FIA_UID.2	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_DES_EXT.1	FPT_FLS.1	FPT_PHP.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1
O.ALARM.FAILURE	x																												
O.AUDIT		x		x	x																					x			
O.CRYPTO						x																							
O.FW.THRESHOLD		x																											
O.FILTER												x	x	x										x					
O.KEY.GENERATE								x																					
O.KEY.LOAD															x														x
O.SELF.TEST			x																					x				x	
O.NO.CONFIG													x						x	x	x								
O.ROBUST.TOE.ACCESS										x	x					x	x	x				x							
O.SECURE.CONFIGURATION										x	x				x												x		x
O.EMERGENCY.ERASE			x						x														x						
O.SECURE.CHANNEL							x																						
NO.SEALING																									x				

Table 4: Mapping of Objectives to SFRs

As it can be seen in Table 4 all objectives are satisfied by at least one SFR and all SFRs are required to meet at least one objective.

6.4.1.1 Security Functional Requirements vs. Objectives

FAU_ARP.1 Security alarms

The TOE will raise a local alarm indication if a TOE hardware or software failure is detected (O.ALARM.FAILURE). (A failure that is reported may compromise the HIGH/LOW protection (O.FILTER).)

FAU_GEN.1 Audit data generation

The TOE registers auditable events indicating type of event and outcome of the event from the TOE (O.AUDIT). The TOE monitors the rate of flow (O.FW.THRESHOLD) through the firewall and issues an audit event if the threshold is exceeded.

FAU_SAA.1 Potential violation analysis

The TOE performs self tests that can detect potential violations (O.SELF.TEST). The TOE has automatic and manual functions for emergency erase (O.EMERGENCY.ERASE)

FAU_SAR.1 Audit review

The TOE provides the capability to read the information from the audit records (O.AUDIT).

FAU_STG.1 Protected audit trail storage

The TOE protects the audit log (O.AUDIT) from deletion and modification of stored events.

FCS_COP.1(1) Cryptographic operation

The TOE performs decryption and strong integrity verification of imported filter configuration files and software update files (O.CRYPTO).

FCS_COP.1(2) Cryptographic operation

The TOE uses asymmetric encryption techniques to establish a secure channel between the TOE and a web client presenting the local management information (O.SECURE.CHANNEL).

FCS_CKM.1 Cryptographic key generation

The TOE generates cryptographic keys for internal use for encryption of imported keys (O.KEY.GENERATE).

FCS_CKM.4 Cryptographic key destruction

The TOE erases cryptographic keys upon tamper detection and manual emergency erase (O.EMERGENCY.ERASE).

FDP_ACC.1 Subset access control

The TOE performs access control of TOE managers (O.ROBUST.TOE.ACCESS) and configuration files in order to ensure secure import of security configuration files (O.SECURE.CONFIGURATION).

FDP_ACF.1 Access control functions

The TOE manager must log in to the TOE with a role and password (O.ROBUST.TOE.ACCESS) and the TOE performs decryption and strong integrity check of configuration files (O.SECURE.CONFIGURATION).

FDP_IFC.2 Complete information flow control

The TOE enforces the firewall filter on all messages sent from the HIGH network to the LOW network (O.FILTER).

FDP_IFF.1 Simple security attributes

The TOE enforces the information flow control SFP based on the attributes of the messages checked by the filter (O.FILTER). The TOE has an information flow control SFP that is non-configurable (O.NO.CONFIG) when it has been loaded into the TOE.

FDP_IFF.6 Illicit information flow monitoring

Messages not complying with the filter specification are rejected and counted (O.FILTER).

FDP_ITC.2 Import from outside of the TOE

The TOE enforces the configuration access control policy when importing filter configuration files and software update files and cryptographic keys from outside the TOE (O.SECURE.CONFIGURATION) and (O.KEY.LOAD)

FIA_ATD.1 User attribute definition

The TOE manager shall have a role (Security operator, Operator) and password (O.ROBUST.TOE.ACCESS).

FIA_UAU.1 User authentication

The TOE manager shall be successfully authenticated by the TOE before allowing any local management functions on behalf of that user (O.ROBUST.TOE.ACCESS).

FIA_UID.2 User identification before any action

Each user shall be successfully identified by the TOE before allowing any other TSF-mediated actions on behalf of that user (O.ROBUST.TOE.ACCESS).

FMT_MSA.1 Management of security attributes

The security attributes are non-configurable (O.NO.CONFIG).

FMT_MSA.3 Static attribute initialization

The security attributes are non-configurable (O.NO.CONFIG).

FMT_SMF.1 Specification of management functions

The TOE manager is able to select diode operation, inject filter configuration files, and to select sets of predefined filter criteria (O.NO.CONFIG).

FMT_SMR.1 Security roles

The TOE maintains roles with access control for the TOE managers (O.ROBUST.TOE.ACCESS).

FPT_DES_EXT.1 Destruction of filter configuration files

The TOE erases filter configuration files upon tamper detection and manual emergency erase (O.EMERGENCY.ERASE).

FPT_FLS.1 Failure with preservation of secure state

The TOE is designed to fail in a safe manner. This includes failure during self-test (O.SELF.TEST) and failure that compromises the HIGH/LOW protection (O.FILTER).

FPT_PHP.1 Passive detection of physical attack

The TOE has sealing (NO.SEALING) to protect the TOE against tampering.

FPT_STM.1 Reliable time stamps

Auditable events are stored with reliable time stamps (O.AUDIT).

FPT_TDC.1 Inter-TSF basic TSF data consistency

The TOE shall consistently interpret the Security configuration files (O.SECURE.CONFIGURATION).

FPT_TST.1 TSF self test

Security critical functions will be tested by a combination of power-up tests, periodic tests, and/or continuous tests (O.SELF.TEST). (A failure detected during this test, may compromise the HIGH/LOW protection (O.FILTER).)

FTP_ITC.1 Inter-TSF trusted channel

The TOE provides a trusted channel (O.SECURE.CONFIGURATION) to a dedicated interface for import of keys (O.KEY.LOAD) for decryption of filter configuration files and software update files.

6.4.1.2 Objectives vs. Security Functional Requirements

O.ALARM.FAILURE

The TOE will raise a local alarm indication (FAU_ARP.1) if a potential security violation is detected due to failure in the TOE.

O.AUDIT

The TOE will generate audit records (FAU_GEN.1) with reliable time stamps (FPT_STM.1) and store the record in a protected storage (FAU_STG.1) that is made available for audit (FAU_SAR.1) by the TOE manager. The TOE monitors the rate of flow through the firewall and issues an audit event (FAU_GEN.1) if the threshold is exceeded.

O.CRYPTO

The TOE performs decryption and strong integrity verification of imported filter configuration files and software update files and performs integrity verification of imported keys (FCS_COP.1(1).

O.FW.THRESHOLD

The TOE shall monitor the flow through the firewall and generate an audit event if the threshold is exceeded (FAU_GEN.1).

O.FILTER

The TOE shall ensure that information transmitted from HIGH domain to LOW domain is unclassified by enforcing the information flow control SFP trough the TOE (FDP_IFC.2). This information flow control SFP is non-configurable (FDP_IFF.1). Messages not complying with the information flow control SFP are rejected counted (FDP_IFF.6) for presentation in the audit log.

The TOE ensures preservation of a secure state after a single failure (FPT_FLS.1).

O.KEY.GENERATE

The TOE shall generate keys for internal use for encryption of imported keys (FCS_CKM.1).

O.KEY.LOAD

The TOE provides a trusted channel to a dedicated interface (FTP_ITC.1) for import of keys (FDP_ITC.2) for decryption of filter configuration files and software update files.

O.SELF.TEST

The TOE ensures that security critical functions are tested by a combination of power-up tests and periodic tests (FPT_TST.1) to detect potential security violations (FAU-SAA.1)

The TOE ensures preservation of a secure state after a single failure (FPT_FLS.1).

O.NO.CONFIG

The TOE filter parameters (FDP_IFF.1) shall not be configurable within the TOE (FMT_MSA.1 and FMT_MSA.3). The TOE manager can select sets of predefined filter criteria (FMT_SMF.1).

O.ROBUST.TOE.ACCESS

The TOE performs access control of TOE managers and configuration files (FDP_ACC.1) and (FDP_ACF.1). The TOE manager is identified by role (Security operator, Operator) and a password (FIA_ATD.1) and shall be fully authenticated before allowing any local management functions on behalf of that user (FIA_UAU.1) and (FIA_UID.2).

O.SECURE.CONFIGURATION

The TOE imports filter configuration files, software update files and cryptographic keys (FDP_ITC.2), and perform access control of the TOE manager (FDP_ACC.1) and (FDP_ACF.1). The TOE will consistently interpret the security configuration files (FPT_TDC.1) and will reject the file if any of the steps fail. The TOE provides a trusted channel to a dedicated interface (FTP_ITC.1) for import of keys.

O.EMERGENCY.ERASE

The TOE has functionality for erasing cryptographic keys (FCS_CKM.4) and filter configuration files (FPT_DES_EXT.1) automatically upon tamper detection and manually from the front panel. This is part of the potential violation analysis (FAU_SAA.1).

O.SECURE.CHANNEL

The TOE uses Transport Layer Security (TLS) on the communication channel with the web client presenting the local management (FCS_COP.1(2).

NO.SEALING

The TOE shall have passive protection (FPT_PHP.1).

6.4.2 Security dependencies are satisfied

Table 5 shows a mapping of Functional Components to their dependencies.

Functional Component	Dependency	Included
TOE Security Functional Requirements		
FAU_ARP.1	FAU_SAA.1	YES
FAU_GEN.1	FPT_STM.1	YES
FAU_SAA.1	FAU_GEN.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FAU_STG.1	FAU_GEN.1	YES
FCS_COP.1(1)	FDP_ITC.1 or	NO
	FDP_ITC.2 or	YES
	FCS_CKM.1	YES
	FCS_CKM.4	YES[2]
FCS_COP.1(2)	FCS_ITC.1 or	NO
	FDP_ITC.2 or	YES
	FCS_CKM.1	YES
	FCS_CKM.4	YES[3]
FCS_CKM.1	FCS_CKM.2 or	NO
	FCS_COP.1	YES
	FCS_CKM.4	YES
FCS_CKM.4	FDP_ITC.1 or	NO
	FDP_ITC.2 or	YES
	FCS_CKM.1	YES
FDP_ACC.1	FDP_ACF.1	YES
FDP_ACF.1	FDP_ACC.1	YES
	FMT_MSA.3	YES
FDP_IFC.2	FDP_IFF.1	YES

[2] Emergency erase

[3] Certificate containing keys are deleted during emergency erase

FDP_IFF.1	FDP_IFC.1	YES[4]
	FMT MSA.3	YES
FDP_IFF.6	FDP_IFC.1	YES[5]
FDP_ITC.2	FDP_ACC.1 or	YES
	FDP_IFC.1	YES[6]
	FTP_ITC.1 or	YES
	FTP_TRP.1	NO
	FPT_TDC.1	YES
FIA_ATD.1	None	
FIA_UAU.1	FIA_UID.1	YES[7]
FIA_UID.2	None	
FMT_MSA.1	FDP_IFC.1 or	YES[8]
	FDP_ACC.1	YES
	FMT.SMR.1	YES
	FMT_SMF.1	YES
FMT_MSA.3	FMT_MSA.1	YES
	FMT_SMR.1	YES
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	YES[9]
FPT_DES_EXT.1	FDP_ITC.1 or	NO
	FDP_ITC.2 or	YES
FPT_FLS.1	None	

[4] FDP_IFF.1 has a dependency to FDP_IFC.1, which is covered by FDP_IFC.2.

[5] FDP_IFF.6 has a dependency to FDP_IFC.1, which is covered by FDP_IFC.2.

[6] FDP_ITC.2 has a dependency to FDP_IFC.1, which is covered by FDP_IFC.2.

[7] FIA_UAU.1 has a dependency to FIA_UID.1, which is covered by FIA_UID.2.

[8] FMT_MSA.1 has a dependency to FDP_IFC.1, which is covered by FDP_IFC.2.

[9] FMT_SMR.1 has a dependency to FIA_UID.1, which is covered by FIA_UID.2.

FPT_PHP.1	None	
FPT_STM.1	None	
FPT_TDC.1	None	
FPT_TST.1	None	
FTP_ITC.1	None	

Table 5: Security Requirements dependencies

6.4.3 SAR rationale

The SARs specified in this ST are according to EAL5 as selected by NSM.

7. TOE SUMMARY SPECIFICATION

7.1 TOE security functions

(1) This describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in chapter 6.2.

7.1.2 SF.Security.Alarm

(1) The TOE will raise a local alarm indication in the following situations:

(2) A firewall test failure is detected in the TOE.

(3) A hardware or software failure is detected in the TOE.

7.1.3 SF.Crypto

(1) The TOE will decrypt filter configuration files and software update files

(2) The TOE will encrypt keys that are imported into the TOE

(3) The TOE will generate keys for internal use

7.1.4 SF.Key.Load

(1) Keys can be imported into the TOE through a dedicated interface and internal channel.

7.1.5 SF.Information.Flow.Control

(1) The information flow control provides flow control between the user interfaces and the HIGH and LOW network and information flow control between the HIGH and LOW network. The flow control rules are based on:

(a) All messages from the HIGH network to the LOW network are filtered in a firewall.

(b) The TOE manager can select sets of predefined filter criteria.

(c) Messages that do not comply with the SFP are rejected.

(d) The number of rejected messages are counted.

7.1.6 SF.Configuration.Access.Control

(1) The configuration access control provides secure import of configuration data by means of access control, integrity, and confidentiality for configuration files. It is based on:

(a) decryption and strong integrity verification of imported filter configuration files,

(b) decryption and strong integrity verification of imported SW update images,

(c) import of keys from a trusted channel,

(d) encryption of internal keys

7.1.7 SF.Access.Control

(1) The TOE has authentication of TOE operators based on ID and password. TOE operators are:

(a) Operator – access to Operator functions,

(b) Security operator – access to Operator and Security operator functions.

7.1.8 SF.Emergency.Erase

(1) Filter configuration files and cryptographic keys are erased automatically upon tamper detection and manually from the front panel.

7.1.9 SF.Secure.Channel

(1) The TOE has a secure channel to the local management

7.1.10 SF.Self.Test

(1) The testing of TOE will detect errors in the security critical functions on the TOE. If a firewall failure or a hardware or software failure is detected in the TOE, an alarm is generated.

7.1.11 SF.Fail.Secure

(1) The most serious violation of the TOE is that classified data on the HIGH network is sent on the LOW network. The following measure shall prevent this to happen as a result of TOE-failures:

(2) The TOE is designed to handle single failures without violating the trusted functionality. In other words: If the TOE fails, it will fail in a safe manner.

7.1.12 SF.Passive.Protection

(1) The TOE has a physical sealing.

7.1.13 SF.Firewall.Treshold

(1) The TOE can monitor the rate of flow of legal messages through the firewall. A threshold value for each legal message can be set in the filter configuration file. The threshold value cannot be changed in the TOE. The TOE generates an audit event when the rate of flow exceeds the threshold value.

7.1.14 SF.Audit.Log

(1) The TOE will record and categorize auditable events in an audit log that is protected from change and deletion. The audit log that can be viewed by authorized users by means of a web browser.

7.2 TOE summary specification rationale

Table 6 shows how TOE Security Functions satisfy SFRs.

TOE Security functions	SFRs	Description
SF.Security.Alarm	FAU_ARP.1	The TOE security alarm function will raise a local alarm upon detection of a hardware failure or software failure in the TOE (FAU_ARP.1).
SF.Crypto	FCS_COP.1(1), FCS_CKM.1.	The TOE performs decryption of filter configuration files and software update files (FCS_COP.1(1)). The TOE generates cryptographic keys (FCS_CKM.1) for encryption FCS_COP.1(1) of imported keys.
SF.Key.Load	FDP_ITC.2, FTP_ITC.1.	Keys can be imported into the TOE (FDP_ITC.2) from a dedicated interface (FTP_ITC.1).
SF.Information.Flow.Control	FDP_IFC.2, FDP_IFF.1, FDP_IFF.6, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1	The TOE information flow control controls all information flows (FDP_IFC.2) determined by the hard coded filter settings (FDP_IFF.1, FMT_MSA.1, and FMT_MSA.3). The TOE manager can select sets of predefined filter criteria (FMT_SMF.1). The TOE monitors number of rejected messages (FDP_IFF.6).

SF.Configuration.Access.Control	FDP_ITC.2, FDP_ACF.1, FPT_TDC.1, FTP_ITC.1.	The TOE performs secure configuration by importing (FDP_ITC.2) encrypted filter configuration files and software update files. The TOE access controls the TOE manager (FDP_ACF.1). The TOE interprets the security configuration files in a consistent manner (FPT_TDC.1). Keys are imported trough a trusted channel (FTP_ITC.1).
SF.Access.Control	FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.2, FMT_SMR.1	The TOE performs access control of TOE managers and configuration files (FDP_ACC.1) and (FDP_ACF.1). The TOE manager shall have a user ID and a password (FIA_ATD.1) and shall be fully authenticated before allowing any local management functions on behalf of that user (FIA_UAU.1) and (FIA_UID.2). The TOE provides different roles for the TOE managers (FMT_SMR.1).
SF.Secure.Channel	FCS_COP.1(2)	The TOE provides a secure channel to the local management.
SF.Emergency.Erase	FAU_SAA.1, FCS_CKM.4, FPT_DES_EXT.1	The TOE erase filter configuration files (FPT_DES_EXT.1) and cryptographic keys (FCS_CKM.4) automatically upon tamper detect (FAU_SAA.) and manually from the front panel.
SF.Self.Test	FAU_SAA.1, FPT_TST.1	The TOE self-test function performs an underlying abstract machine testing (FPT_TST.1) and makes an analysis if there has been a security violation (FAU_SAA.1) that shall cause a halt or a reboot.
SF.Fail.Secure	FPT_FLS.1	The fail secure function preserves a secure state after failure by shutting down the Ethernet interfaces and restarting the unit (FPT_FLS.1).
SF.Passive.Protection	FPT_PHP.1	The TOE sealing is constructed so that physical tampering is easily discovered (FPT_PHP.1).
SF.Audit.Log	FAU_GEN.1, FAU_STG.1, FAU_SAR.1, FPT_STM.1	The TOE audit log function record auditable events (FAU_GEN.1) in an audit log. The stored events cannot be modified or deleted (FAU_STG.1). The audit log can be viewed by authorized users (FAU_SAR.1) on the HIGH network. The auditable events are stored with a reliable time stamp (FPT_STM.1).
SF.Firewall.Threshold	FAU_GEN.1	The TOE firewall threshold function monitors the rate of flow through the firewall and generates an audit if the threshold is exceeded (FAU_GEN.1).

Table 6: TOE Security Functions satisfy SFRs

(1) Strength of TOE security function analysis shall be performed on probabilistic or permutational functions.

(2) The TOE does not have any probabilistic or permutational functions. Hence, there are no TOE security functions having a TOE security function claim and there is no further strength of TOE security function analysis required.

8. NOTES

8.1 Acronyms and Abbreviations

CC	Common Criteria
CI	Controlled Item
CIK	Crypto Ignition Key
EAL	Evaluation Assurance Level
FW	Firewall
HW	Hardware
IP	Internet Protocol
IT	Information Technology
KAT	Known Answer Test
LAN	Local Area Network
NAT	Network Address Translation
NSM	Nasjonal sikkerhetsmyndighet
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement(s)
SOF	Strength of Function
ST	Security Target
SW	Software
TLS	Transport Layer Security
TOE	Target of evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSF 201	Trusted Security Filter (product name)
TSP	TOE Security Policy

8.2 Definitions

Classified information	Classified information is information regarded as sensitive by the security authorities for the owners of the system that comprises the TOE. Sensitive information is information that these security authorities determine must be protected because its unauthorised disclosure will cause perceivable damage.
HIGH domain (red)	The domain that handles the higher classified information in clear.
LOW domain (black)	The domain that handles the lower classified information in clear. If this domain is defined as unclassified, only unclassified information shall be allowed in this domain.