# Security Target for the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS 2.80 CC Compliant Firmware: EAL4+

**Document No. 1476-011-D001**

Version 0.90, 2 February 2005

*Prepared for:*

**Fortinet, Incorporated**
1688 Woodward Drive
Ottawa, Ontario
Canada  K2C 3R8

*Prepared by:*

**Electronic Warfare Associates-Canada, Ltd.**
55 Metcalfe St., Suite 1600
Ottawa, Ontario
K1P 6L5

# Security Target for the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS 2.80 CC Compliant Firmware: EAL4+

**Document No. 1476-011-D001**

Version 0.90, 2 February 2005

<Original> Approved by:

Project Engineer: S. Moore ______

Project Manager: E. Connor ______

Program Director: P. Zatychec ______

(Signature) (Date)

# TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

# 1 INTRODUCTION

## 1.1 IDENTIFICATION

This document is the Security Target (ST) for the FortiGate™ Antivirus Firewalls detailed in Table 1.

| Product | Firmware[1] Version | Hardware Version[2] |
|---|---|---|
| FortiGate-50A | Fortigate-50A 2.80, build275,050127 | C-5FA27-01 |
| FortiGate-60 | Fortigate-60 2.80, build275,050127 | C-4AN27-03 |
| FortiGate-100A | Fortigate-100A 2.80, build275,050127 | C-4DZ47-01 |
| FortiGate-200A | Fortigate-200A 2.80, build275,050127 | C-4AY89-01 |
| FortiGate-300A | Fortigate-300A 2.80, build275,050127 | C-4FK88-01 |
| FortiGate-800 | Fortigate-800 2.80, build275,050127 | C-4UT39-01 |
| FortiGate-3000 | Fortigate-3000 2.80, build275,050127 | C-4JE25-02 |
| FortiGate-3600 | Fortigate-3600 2.80, build275,050127 | C-4KW75-02 |
| FortiGate-5001 | Fortigate-5000 2.80, build275,050127 | P-4CF76-01 |

**Table 1 - TOE Identification Details**

These products are collectively termed the FortiGate Series or FortiGate Antivirus Firewalls.

Documentation for FortiGate units operated in Common Criteria mode consists of the standard FortiOS version 2.80 MR5 documentation set plus a CC-specific technical note.

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, August 1999, CCIMB-99-031, annotated with interpretations as of 2003-12-31.

[1] The firmware is assigned a version number that is identical to the version number of the software that is loaded onto it. The firmware version number is shown here because the operational program for the FortiGate series is stored in firmware.

[2] For the purposes of the ST, only the first 3 fields of the hardware version are relevant. The complete version includes a field for non-CC relevant changes and a padding field for compatibility with other Fortinet version naming conventions.

## 1.2 OVERVIEW

The FortiGate Series is a series of hardware firewalls designed to protect computer networks from abuse. They reside between the network they are protecting and an external network such as the internet. The FortiGate Series spans the full range of network environments, from the small office and home office (SOHO) to service provider, offering cost-effective systems for any application. They detect and eliminate damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content, etc. in real-time without degrading network performance. In addition to providing application-level protection, the FortiGate Series deliver a full range of network-level services which include firewall, Virtual Private Network (VPN), intrusion prevention and traffic shaping in dedicated, easily managed platforms. The FortiGate series provides a NAT/route mode that applies security features between two or more different networks (for example, between a private network and the Internet) and a transparent mode that applies security features at any point in a network.

Each FortiGate unit consists of a hardware box and the custom firewall software FortiOS™. A separate administrator console is used to perform system administration. The firewall can operate either alone or as part of a firewall cluster in order to provide high availability of services. The models offered in the FortiGate Series share common software. The different models in the series provide for increased performance and additional protected ports.

## 1.3 CC CONFORMANCE

The FortiGate Antivirus Firewall is conformant with the identified functional requirements specified in Part 2 of the CC. The FortiGate unit is conformant to the assurance requirements for Evaluation Assurance Level (EAL) 4, as specified in Part 3 of the CC, with the following augmentation:

- ALC_FLR.3 – Systematic Flaw Remediation

The Target of Evaluation (TOE) for this ST is conformant with the following Protection Profile (PP):

- U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999 (TFFWLR PP)

## 1.4 CONVENTIONS

### 1.4.1 Operations

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets and italicised text, e.g., [*selected item*].

- Assignment: Indicated by surrounding brackets and regular text, e.g., [assigned item].

- Refinement: Indicated by underlined text, e.g., refined item for additions or strikethrough text, e.g., ~~refined item~~ for deleted items.

- Iteration: Indicated by assigning a number at the functional component level, e.g., “FDP_ACC.1(1), Subset access control” and “FDP_ACC.1(2) Subset access control”.

The markings are relative to the requirements statement in the CC. Deviations in phrasing that are required for compliance with the PP are noted, either as footnotes or as entries in the rationale.

### 1.4.2 Order of Presentation

This ST distinguishes assumptions, threats, objectives, and requirements that are taken from the TFFWLR PP from additional information by placing them in separate subsections. For example, the Assumptions Section is subdivided into “Assumptions Listed in TFFWLR PP” and “Additional Assumptions”. The TFFWLR PP material is presented first.

## 1.5 TERMINOLOGY

The following terminology is used in this ST:

Attack Potential
The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker’s expertise, resources and motivation.

Controlled Subject
Entity under control of the TOE Security Policy (TSP).

Presumed Address
The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Therefore, a "presumed address" is used to identify source and destination addresses.

# 2 TARGET OF EVALUATION DESCRIPTION

## 2.1 PHYSICAL DESCRIPTION

The FortiGate Series is a set of antivirus firewalls that are used to control network access. They implement the classic firewall capability of perimeter security, in which they control the transfer of data between two networks, one considered to be "external" to the assets that are to be protected and the second considered to be "internal" to these assets. This concept is extended in some FortiGate Series models to control access between multiple networks or network segments. Figure 1 shows an example of a FortiGate Antivirus Firewall protecting an internal network and also providing a second network, termed the Demilitarized Zone (DMZ) that is isolated from both the external network and the internal network. The TOE consists of the FortiGate Antivirus Firewall. The FortiGate units are designed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.

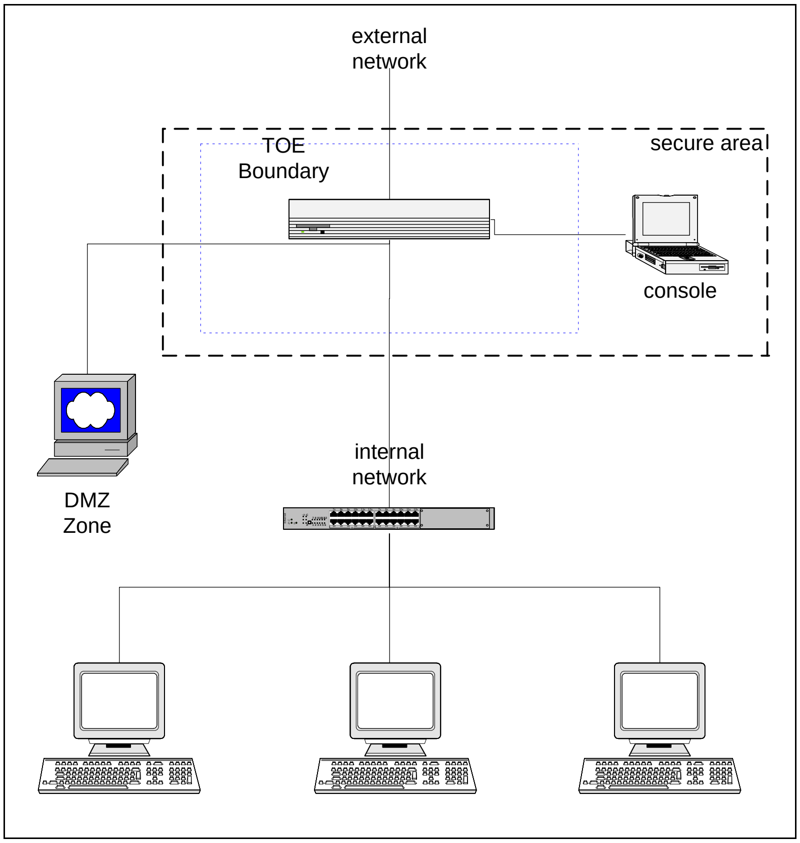

**Figure 1 - Typical FortiGate Antivirus Firewall Network Configuration**

### 2.1.1 Architecture Model

Each member of the FortiGate Series consists of custom hardware and software. All models share a common software platform and use a proprietary Application-Specific Integrated Circuit (FortiASIC™) to improve performance. The FortiASIC performs security and content processing. The FortiGate unit consists of the following major components: FortiOS which includes the firewall engine and management software, processor, memory, FortiASIC, I/O interfaces, and hard drive on some models. Some models offer dual processor and FortiASIC combinations in order to increase performance.

The FortiGate units have the interfaces defined in Table 2.

| | **Interfaces** | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **Internal**[3] | **External**[3] | **DMZ**[3] | **Console** | **Control Panel** | **USB**[4] |
| FortiGate-50A | 1 | 1 | None | RS232/DB-9 | None | 2 |
| FortiGate-60 | 4 | 2 | 1 | RS232/DB-9 | None | 2 |
| FortiGate-100A | 1 | 1 | 1 | RS232/DB-9 | None | None |
| FortiGate-200A | 1 | 1 | 1 | RS232/DB-9 | 4 button with LCD | None |
| FortiGate-300A | 1 | 1 | 1 | RS232/DB-9 | 4 button with LCD | None |
| FortiGate-800 | user definable, 4 x 10/100<br>user definable, 4 x 10/100/1000 | | | RS232/RJ-45 | 4 button with LCD | Not used |
| FortiGate-3000 | 1 | 1 | N/A | RS232/DB9 | 4 button with LCD | None |
| | user definable, 3x10/100, 1x1000 | | | | | |
| FortiGate-3600 | 1 | 1 | NA | RS232/DB-9,<br>RS232/RJ-45 | 4 button with LCD | None |
| | user definable, 4 x 1000 | | | | | |
| FortiGate-5001 | user definable, 4 x Gigabit Fiber<br>user definable, 4 x 10/100/1000 | | | RS232/DB-9 | None | 2 (future use) |

**Table 2 - FortiGate Anitvirus Firewall Interfaces**

The FortiGate-5001 is an antivirus firewall module (blade) that may be installed in the FortiGate-5020, 5050 or 5140 chassis, each of which is capable of holding multiple blades. The chassis provides mounting, power and cooling fans only. As network and management interfaces are part of the blade itself, each blade acts as an independent antivirus firewall.

[3] Number of Ethernet ports. Speed is 10/100 Mbps unless specified.

[4] USB is the abbreviation for Universal Serial Bus.

## 2.2 LOGICAL DESCRIPTION

### 2.2.1 Features Included In TOE

The FortiGate Antivirus Firewall performs the following security functions:

#### 2.2.1.1 Access Control

The FortiGate Antivirus Firewall provides a role-based access control capability to ensure that only authorized administrators are able to administer the FortiGate unit. Internal network users who wish to pass information through the FortiGate unit are not required to authenticate to the FortiGate unit, but are subject to access control based on their IP address.

#### 2.2.1.2 Information Flow Control

The FortiGate Antivirus Firewall implements stateful inspection. Information flow is restricted to that permitted by a set of rules that are defined by the Administrator.

#### 2.2.1.3 Logging

Logging is performed and data is either stored in memory or written to hard disk. Events that are recorded consist of the following:

- Administrative Events, such as system configuration changes
- Network anomalies, which may be associated with attacks
- Traffic Events, associated with session establishment and packet information flow

#### 2.2.1.4 Administration

Depending on the model the FortiGate Antivirus Firewall provides the following administration options:

- On all models a dedicated console port is available. The port is RS232 with either a DB-9 or RJ-45 connector. When connected to an appropriate terminal the console port allows access to the FortiGate unit via a Command Line Interface (CLI). This CLI permits an authorized administrator to configure the FortiGate unit, monitor its operation and examine the audit logs that are created.
- On the 200A, 300A, 800, 3000 and the 3600, basic administration can be performed using the control panel’s LCD and control buttons. The control panel can be used to set the interface IP address, default gateway, and to select network address translation (NAT) or transparent (TP) mode.

- On all models a direct x-over Ethernet cable can be connected to an Ethernet port that has been configured for administrative use. When connected to an appropriate computer this port provides direct local access to the CLI and to the GUI and allows an authorized administrator to configure the Fortigate Unit, monitor its operation, examine the audit logs that are created, and perform backup and archive activities.

### 2.2.2 Features Excluded From TOE

#### 2.2.2.1 VPN

The FortiGate Series supports Virtual Private Networking (VPN) to provide a secure connection between widely separated office networks or securely link telecommuters or travellers to an office network.

#### 2.2.2.2 Anti-Virus Protection

The FortiGate Series provides antivirus protection for web HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), and email (Simple Mail Transfer Protocol (SMTP), Post-Office Protocol Version 3 (POP3), and Internet Message Access Protocol (IMAP)) content as it passes through the FortiGate unit. The FortiGate unit can be configured for the automatic update of the virus data definition file.

#### 2.2.2.3 Web Filtering

Web content filtering can be configured to scan and block all HTTP content protocol streams for Uniform Resource Locators (URLs) or for web page content.

#### 2.2.2.4 Email Filtering

Email filtering can be configured to scan all IMAP and POP3 email content for unwanted senders or for unwanted content.

#### 2.2.2.5 Logging and Reporting

The FortiGate Series remote administration GUI provides additional logging and reporting that is not required to address the TOE Security Functions (TSF).

#### 2.2.2.6 Intrusion Prevention

The FortiGate units incorporate an Intrusion Prevention System (IPS) that detects and prevents suspicious network activity in real time. The IPS uses attack signatures to identify over 1300 attacks. The IPS definitions can be updated manually or the FortiGate unit can be configured to automatically download updates.

#### 2.2.2.7 Traffic Shaping

The FortiGate unit can be configured to restrict traffic based on bandwidth and time.

### 2.2.3 Features Not Supported

The FortiGate Series provides a high availability capability which provides for fall-over between two or more units.  As the TOE consists of one FortiGate unit this feature is not supported in the evaluated configuration.

## 2.3 TOE SECURITY FUNCTIONAL POLICIES

This Security Target references a single information flow control Security Function Policy (SFP), called the UNAUTHENTICATED SFP. The subjects under control of this policy are the TOE interfaces that connect to external IT entities on an internal or external network sending information through the TOE to other external IT entities. The information flowing between subjects in the policy is traffic with attributes, defined in FDP_IFF.1.1, including source and destination addresses. The rules that define the SFP are found in FDP_IFF.1.2. FMT_MSA.3 requires that these rules be assigned restrictive initial values.  FMT_MSA.1 ensures that the rules are subsequently managed only by the authorized administrator.

# 3 TOE SECURITY ENVIRONMENT

## 3.1 ASSUMPTIONS

### 3.1.1 General

The TFFWLR PP states that TFFWLR PP-compliant TOEs are intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent. The language is clearly aimed at government environments.

FortiGate Antivirus Firewalls are also intended to be used in the commercial environment, in which it is important to control the flow of information between two networks or network segments. In keeping with the TFFWLR PP nomenclature, these are termed internal and external networks. The internal network has access to the information of highest value, which the firewall isolates from the external network, an example of which is the Internet.

### 3.1.2 Assumptions Listed in TFFWLR PP

The following conditions are assumed by the TFFWLR PP to exist in the operational environment:

A.PHYSEC The TOE is physically secure.

A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.PUBLIC The TOE does not host public data.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

A.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

A.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

A.REMACC Authorized administrators may access the TOE remotely from the internal and external networks[5].

### 3.1.3 Additional Assumptions

The following additional conditions are assumed to exist in the operational environment:

[5] The PP explicitly allows this capability to be optional. While remote administrator access could be allowed, the TOE does not provide any support for this feature.

| | |
|---|---|
| A.HIGHEXP | The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered high. |
| A.CONSOLE | A securely-configured management console, in the same physically-secure location as the TOE, is directly connected to the TOE via a dedicated link entirely within a controlled area of the environment. The console is expected to correctly transmit the information entered on it to the TOE; and to correctly display the information sent to it by the TOE. |
| A.CONSOLE_ACCESS | Access to the console will be restricted to authorized administrators. |

## 3.2 THREATS

### 3.2.1 Threats Listed in TFFWLR PP

#### 3.2.1.1 Threats Addressed by TOE

The threats discussed below are addressed by Protection Profile-compliant TOEs. The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself. The threat agent is assumed to be an independent attacker with a low-level of sophistication who is attacking simply for the thrill of doing so, without a specific agenda. The resources are assumed to include only those attack tools that are publicly available.

| | |
|---|---|
| T.NOAUTH | An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE. |
| T.REPEAT | An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE. |
| T.REPLAY | An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE. |
| T.ASPOOF | An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network ~~by using~~ uses[6] a spoofed source address. |
| T.MEDIAT | An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network. |
| T.OLDINF | Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE. |

[6] The wording was changed from the PP in order to provide a complete sentence. The meaning was not changed.

| | |
|---|---|
| T.PROCOM[7] | An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE. |
| T.AUDACC | Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection. |
| T.SELPRO | An unauthorized person may read, modify, or destroy security critical TOE configuration data. |
| T.AUDFUL | An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions. |

#### 3.2.1.2 Threat To Be Addressed by the Operating Environment

The threat possibility discussed below must be countered by procedural measures and/or administrative methods.

| | |
|---|---|
| T.USAGE | The TOE may be inadvertently delivered, configured, used and administered in an insecure manner by either authorized or unauthorized persons. |

### 3.2.2 Additional Threats

None.

## 3.3 ORGANISATIONAL SECURITY POLICIES

The TOE is not intended for use by a specific organization or type of organization. There is also no need for the TOE to implement a set of rules that cannot be sensibly included within or implied by a threat description. The security objectives are therefore derived solely from threats and assumptions and no organisational security policies are included.

[7] The TOE does not allow administration to occur remotely from a connected network, so this threat is not applicable. It is included to ensure completeness with the PP.

# 4 SECURITY OBJECTIVES

## 4.1 SECURITY OBJECTIVES FOR THE TOE

### 4.1.1 Security Objectives for the TOE Listed in the TFFWLR PP

The following are the IT security objectives for the TOE stated in the TFFWLR PP:

O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.

O.SINUSE[8] The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.

O.MEDIAT The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.

O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

O.ENCRYP[9] The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.

O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

[8] The TOE does not allow administration to occur remotely from a connected network, so this objective is not applicable. It is included to ensure completeness with the PP.

[9] The TOE does not allow administration to occur remotely from a connected network, so this objective is not applicable. It is included to ensure completeness with the PP.

For a detailed mapping between threats and the IT security objectives listed above see Section 8.1.1 of the Rationale.

### 4.1.2 Additional Security Objectives for the TOE

None.

## 4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

### 4.2.1 Security Objectives for the Environment Listed in the TFFWLR PP

The TFFWLR PP considers all of the assumptions stated in section 3.1 to be security objectives for the environment. These assumptions, with names changed from ”A.x” to “O.x” are stated below. The TFFWLR PP includes two security objectives, O.GUIDAN and O.ADMTRA, which are stated below. These are non-IT security objectives, which are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

O.PHYSEC The TOE is physically secure.

O.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

O.PUBLIC The TOE does not host public data.

O.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

O.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

O.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

O.NOREMO[10] Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

O.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

O.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.

For a detailed mapping between threats, assumptions, and the non-IT security objectives listed above see Section 8.1 of the Rationale.

[10] The PP indicates that remote administration is an objective of the non-IT security environment of the TOE, and allows this capability to be optional. This objective is included here to allow a complete mapping of the PP to this ST. The TOE does not provide any support for these features.

### 4.2.2 Additional Security Objectives for the Environment

O.HIGHEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered high.

O.NOREMACC Authorized administrators are not able to access the TOE remotely from the internal and external networks.

O.CONSOLE A management console, configured in accordance with the administrative guidance, is directly connected to the TOE via a dedicated link entirely within a controlled area of the environment. The console is in the same physical location as the TOE and is physically secure. The console is expected to correctly transmit the information entered on it to the TOE and to correctly display the information sent to it by the TOE.

O.CONSOLE_ACCESS Access to the console will be restricted to authorized administrators.

# 5 IT SECURITY REQUIREMENTS

## 5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

### 5.1.1 Overview

#### 5.1.1.1 Content

The security functional requirements for this ST consist of the following components from Part 2 of the CC, summarized in Table 3.

Every SFR included in the Protection Profile (TFFWLR PP) identified in the Protection Profile Claims section is addressed in this ST. Each SFR from the TFFWLR PP was copied, changed in this ST to complete operations left incomplete by the TFFWLR PP or to make necessary refinements to preserve the intent of the TFFWLR PP. International Interpretations, as of 2003-12-31, have been incorporated by changing the SFRs as required.

| CC Part 2 Security Functional Components | | |
|---|---|---|
| **Identifier** | **Name** | **Notes** |
| FAU_GEN.1 | Audit data generation | As remote administration is not supported by the TOE, references to remote administration have been removed. |
| FAU_SAR.1 | Audit review | |
| FAU_SAR.3 | Selectable audit review | |
| FAU_STG.1 | Protected audit trail storage | |
| FAU_STG.4 | Prevention of audit data loss | |
| FCS_COP.1 | Cryptographic operation | As the TOE does not support remote administration, this requirement does not apply. It has therefore been omitted from this section along with the removal of the FAU_GEN.1 reference to this component. |
| FDP_IFC.1 | Subset information flow control | |
| FDP_IFF.1 | Simple security attributes | |
| FDP_RIP.1 | Subset residual information protection | |
| FIA_AFL.1 | Authentication failure handling | As the TOE does not support an interface where a non-administrator can attempt to authenticate itself to the TOE (e.g., for remote administration), this requirement does not apply. It has therefore been omitted from this section along with the removal of the FAU_GEN.1 and FMT_MOF.1 references to this component. |
| FIA_ATD.1 | User attribute definition | |

| CC Part 2 Security Functional Components | | |
|---|---|---|
| **Identifier** | **Name** | **Notes** |
| FIA_SOS.1 | Specification of secrets | As the TOE does not support an interface where a non-administrator can attempt to authenticate itself to the TOE (e.g., for remote administration), no audit data is generated for the rejection of any tested secret by the TSF. |
| FIA_UAU.1 | Timing of authentication | |
| FIA_UAU.4 | Single-use authentication mechanisms | As the TOE does not support remote administration, where replay might be relevant, this requirement does not apply. It has therefore been omitted from this section along with the removal of the FMT_MOF.1 references to this component. |
| FIA_UID.2 | User identification before any action | |
| FMT_MOF.1 | Management of security functions behavior | As remote administration is not supported by the TOE, related restrictions have been removed from this requirement. |
| FMT_MSA.1 | Management of security attributes | |
| FMT_MSA.3 | Static attribute initialization | |
| FMT_SMF.1 | Specification of Management Functions | This requirement has been added as a result of Interpretation 065. The FMT_MOF.1 functions have been included in this requirement. |
| FMT_SMR.1 | Security roles | |
| FPT_RVM.1 | Non-bypassability of the TSP | |
| FPT_SEP.1 | TSF domain separation | |
| FPT_STM.1 | Reliable time stamps | |

**Table 3 - Summary of CC Part 2 Security Functional Requirements**

#### 5.1.1.2 Strength of Function

The minimum strength level for the TOE security functions realized by a probablistic or permutational mechanism shall be SOF-basic. The rationale for this selected level is presented in Section 8.5.

Specific strength of function metrics are defined for the following requirements:

FIA_UAU.1 Strength of Function shall be demonstrated such that the probability that authentication data can be guessed is no greater than one in one million (0.000001).

### 5.1.2 Security Functional Requirements

#### 5.1.2.1 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:

a) Start-up and shutdown of the audit functions;

b) All relevant auditable events for the [*minimal or basic level of audit*[11] *specified in Table 4*]; and

c) [the event in Table 4 listed at the "extended" level].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subjects’ identit~~y~~ies, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [information specified in column four of Table 4].

| Functional Component | Level | Auditable Event | Additional Audit Record Contents |
|---|---|---|---|
| FDP_IFF.1 | Basic | All decisions on requests for information flow. | The presumed addresses of the source and destination subject. |
| FIA_UAU.1 | Basic | Any use of the authentication mechanism. | The user identities provided to the TOE |
| FIA_UID.2 | Basic | All use of the user identification mechanism | The user identities provided to the TOE |
| FMT_MOF.1 | Extended | Use of the functions listed in this requirement pertaining to audit. | The identity of the authorized administrator performing the operation |
| FMT_SMR.1 | Minimal | Modifications to the group of users that are part of the authorized administrator role. | The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role |
| FPT_STM.1 | Minimal | Changes to the time. | The identity of the authorized administrator performing the operation and the new time. |

Table 4 - Auditable Events

[11] The wording for this requirement was taken from the PP. Interpretation 202 limits the level of audit to one of: minimum, basic, detailed, not specified. The intent of the PP author was to specify the level of audit per requirement rather than one overall level. In the context of interpretation 202, the PP author has selected “minimum”, which the PP calls “minimal”, and has then refined the requirement with a higher level of audit in some cases.

### 5.1.2.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

### 5.1.2.3 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [*searches and sorting*] of audit data based on:

a) [presumed subject address;

b) ranges of dates;

c) ranges of times; and

d) ranges of addresses].

### 5.1.2.4 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[12] modifications to the audit records in the audit trail.

### 5.1.2.5 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [*prevent auditable events, except those taken by the authorized administrator ~~user with special rights~~*] and [shall limit the number of audit records lost] if the audit trail is full.

### 5.1.2.6 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [UNAUTHENTICATED SFP] on:

a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;

b) information: traffic sent through the TOE from one subject to another; and

c) operations: pass information].

[12] The insertions to the element are a result of Interpretations 141 and 202.

### 5.1.2.7 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [UNAUTHENTICATED SFP] based on at least the following types of subject and information security attributes:

a) [subject security attributes:

- presumed address;
- [and no additional attributes.]

b) information security attributes:

- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service;
- [and schedule, defined by days of the week and start/stop time]].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and another controlled ~~information~~ subject[13] via a controlled operation if the following rules hold:

a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all

[13] This SFR has been refined to match the PP which specifies that the information flow is between two subjects.

possible combinations of the values of the information flow security attributes, created by the authorized administrator;

- the presumed address of the source subject, in the information, translates to an external network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.3 The TSF shall enforce the [none].

FDP_IFF.1.4 The TSF shall provide the following [none].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:

a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network; and

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.]

### 5.1.2.8 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*allocation of the resource to*] the following objects: [resources that are used by the subjects of the TOE to communicate through the TOE to other subjects].

Application Note: If, for example, the TOE pads information with bits in order to properly prepare the information before sending it out an interface, these bits would be considered a "resource". The intent of the requirement is that these bits shall not contain the remains of information that had previously passed through the TOE. The requirement is met by overwriting or clearing resources, (e.g. packets) before making them available for use.

### 5.1.2.9 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) [identity;

b) association of a human user with the authorized administrator role;

c) [and access profile, which identifies the group of access privileges accorded to the user.]].

### 5.1.2.10 FIA_SOS.1(1) Specification of secrets (CLI/GUI)

FIA_SOS.1(1).1 The TSF shall provide a mechanism to verify that secrets meet [a minimum length of eight (8) characters for administrators accessing the TSF via the CLI or GUI interfaces].

### 5.1.2.11 FIA_SOS.1(2) Specification of secrets (LCD)

FIA_SOS.1(2).1 The TSF shall provide a mechanism to verify that secrets meet [a minimum length of six (6) digits for administrators accessing the TSF via the LCD interface].

### 5.1.2.12 FIA_UAU.1 Timing of authentication[14]

FIA_UAU.1.1 The TSF shall allow [user identification as stated in FIA_UID.2] on behalf of the ~~user~~ authorized administrator ~~or authorized external IT entity~~ accessing the TOE to be performed before the ~~user~~ authorized administrator ~~or authorized external IT entity~~ is authenticated.

FIA_UAU.1.2 The TSF shall require each ~~user~~ authorized administrator ~~or authorized external IT entity~~ to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that ~~user~~ authorized administrator ~~or authorized IT entity~~.

### 5.1.2.13 FIA_UID.2(1) User identification before any action (CLI/GUI)

FIA_UID.2(1).1 The TSF shall require each user to identify itself by entering a username on the CLI or GUI before allowing any other TSF-mediated actions that are invoked through the CLI or GUI on behalf of that user.

[14] As the TOE does not provide support for remote administration, the TOE does not provide any support for the deleted features.

### 5.1.2.14 FIA_UID.2(2) User identification before any action (LCD)

FIA_UID.2(2).1 The TSF shall require each user to identify itself by accessing the LCD before allowing any other TSF-mediated actions that are invoked through the LCD panel on behalf of that user.

Note: The TOE assumes that only the administrator has access to the LCD.

### 5.1.2.15 FMT_MOF.1 Management of security functions behavior[15]

FMT_MOF.1.1 The TSF shall restrict the ability to [*perform*] the functions:

a) [{start-up and shutdown;

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;

~~d) enable and disable single-use authentication mechanisms in FIA_UAU.4 (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);~~

~~e) modify and set the threshold for the number of permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);~~

~~f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);~~

~~g) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);~~

h) modify and set the time and date;

i) archive, create, delete, empty, and review the audit trail;

j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;

k) recover to the state following the last backup;

[15] As the TOE does not provide support for remote administration, the TOE does not provide any support for the deleted features.

~~l) additionally, if the TSF supports remote administration from either an internal or external network:~~

- ~~enable and disable remote administration from internal and external networks;~~
- ~~restrict addresses from which remote administration can be performed;~~

m) [and no other functions]].

to [an authorized administrator].

#### 5.1.2.16 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [UNAUTHENTICATED SFP] to restrict the ability to [*change_default*, *query*, *modify*, *delete*] the security attributes [defined in FDP_IFF.1.1] to the [authorized administrator].

#### 5.1.2.17 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [UNAUTHENTICATED SFP] to provide [*restrictive*] default values for information flow security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

Application Note: The default values for the information flow control security attributes appearing in FDP_IFF.1 are intended to be restrictive in the sense that both inbound and outbound information is denied by the TOE until the default values are modified by an authorized administrator.

#### 5.1.2.18 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a) [start-up and shutdown

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows.

c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;

d) modify and set the time and date;

e) archive, create, delete, empty, and review the audit trail;

f) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools; and

g) recover to the state following the last backup].

#### 5.1.2.19 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the role~~s~~ [authorized administrator].

FMT_SMR.1.2 The TSF shall be able to associate human users with the authorized administrator role~~s~~.

#### 5.1.2.20 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

#### 5.1.2.21 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

#### 5.1.2.22 FPT_STM.1 Reliable time stamps

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

Application Note: The word "reliable" in the above requirement means that the order of the occurrence of auditable events is preserved. Reliable time stamps, which include both date and time, are especially important for TOEs comprised of greater than one component.

## 5.2 TOE SECURITY ASSURANCE REQUIREMENTS

### 5.2.1 Overview

The security assurance requirements for the TOE consist of the requirements corresponding to the EAL4 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw Remediation.

The assurance components are summarized in the following table:

| **Assurance Class** | **Assurance Components** | |
|---|---|---|
| | **Identifier** | **Name** |
| Configuration Management | ACM_AUT.1 | Partial CM automation |
| | ACM_CAP.4 | Generation support and acceptance procedures |
| | ACM_SCP.2 | Problem tracking CM coverage |
| Delivery and Operation | ADO_DEL.2 | Detection of modification |
| | ADO_IGS.1 | Installation, generation, and start-up procedures |

| Assurance Class | Assurance Components | |
|---|---|---|
| | Identifier | Name |
| Development | ADV_FSP.2 | Fully defined external interfaces |
| | ADV_HLD.2 | Security enforcing high-level design |
| | ADV_IMP.1 | Subset of the implementation of the TSF |
| | ADV_LLD.1 | Descriptive low-level design |
| | ADV_RCR.1 | Informal correspondence demonstration |
| | ADV_SPM.1 | Informal TOE security policy model |
| Guidance Documents | AGD_ADM.1 | Administrator guidance |
| | AGD_USR.1 | User guidance |
| Life Cycle Support | ALC_DVS.1 | Identification of security measures |
| | ALC_FLR.3 | Systematic flaw remediation |
| | ALC_LCD.1 | Developer defined life-cycle model |
| | ALC_TAT.1 | Well-defined development tools |
| Tests | ATE_COV.2 | Analysis of coverage |
| | ATE_DPT.1 | Testing: high-level design |
| | ATE_FUN.1 | Functional Testing |
| | ATE_IND.2 | Independent testing – sample |
| Vulnerability Assessment | AVA_MSU.2 | Validation of analysis |
| | AVA_SOF.1 | Strength of TOE security function evaluation |
| | AVA_VLA.2 | Independent vulnerability analysis |

**Table 5 - EAL4 Assurance Requirements**

### 5.2.2 Assurance Requirements

#### 5.2.2.1 ACM_AUT.1 Partial CM automation

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.2.2.2 ACM_CAP.4 Generation support and acceptance procedures

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labelled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.newC[16] The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

[16] The CC does not contain an identifier for this assurance requirement, which was added as a result of Interpretation 003. A unique identifier was therefore created.

### 5.2.2.3 ACM_SCP.2 Problem tracking CM coverage

ACM_SCP.2.1D The developer shall provide a list of configuration items for the TOE.

ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.2.2.4 ADO_DEL.2 Detection of modification

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.2.2.5 ADO_IGS.1 Installation, generation, and start-up procedures

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

### 5.2.2.6 ADV_FSP.2 Fully defined external interfaces

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

#### 5.2.2.7 ADV_HLD.2 Security enforcing high-level design

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

### 5.2.2.8 ADV_IMP.1 Subset of the implementation of the TSF

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

### 5.2.2.9 ADV_LLD.1 Descriptive low-level design

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

### 5.2.2.10 ADV_RCR.1 Informal correspondence demonstration

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.2.2.11 ADV_SPM.1 Informal TOE security policy model

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.2.2.12 AGD_ADM.1 Administrator guidance

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 5.2.2.13 AGD_USR.1 User guidance

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 5.2.2.14 ALC_DVS.1 Identification of security measures

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

#### 5.2.2.15 ALC_FLR.3 Systematic flaw remediation

ALC_FLR.3.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.3.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.3.3D The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.3.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.3.5C The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.3.6C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.3.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.3.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

ALC_FLR.3.9C The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

ALC_FLR.3.10C The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.

ALC_FLR.3.11C The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

ALC_FLR.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 5.2.2.16 ALC_LCD.1 Developer defined life-cycle model

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 5.2.2.17 ALC_TAT.1 Well-defined development tools

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.2.2.18 ATE_COV.2 Analysis of coverage

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.2.2.19 ATE_DPT.1 Testing: high-level design

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

ATE_DPT.1.2E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.2.2.20 ATE_FUN.1 Functional Testing

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 5.2.2.21 ATE_IND.2 Independent testing – sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

#### 5.2.2.22 AVA_MSU.2 Validation of analysis

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

#### 5.2.2.23 AVA_SOF.1 Strength of TOE security function evaluation

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the ST.

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

#### 5.2.2.24 AVA_VLA.2 Independent vulnerability analysis

AVA_VLA.2.1D The developer shall perform a vulnerability analysis.

AVA_VLA.2.2D The developer shall provide vulnerability analysis documentation.

AVA_VLA.2.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.2.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.2.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

| | |
|---|---|
| AVA_VLA.2.4E | The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment. |
| AVA_VLA.2.5E | The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential. |

## 5.3 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

None.

# 6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements defined in Section 5. The functions and functional requirements are cross-referenced in Table 11. The assurance measures and assurance requirements are cross-referenced in Table 12.

## 6.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

F.HMI The TOE provides the administrator with the capability to perform HMI functions including:

a) start-up and shutdown;

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) create, delete, modify, and view user attribute values (identity; association of a human user with the authorized administrator role and access profile).

d) modify and set the time and date;

e) archive, create, delete, empty, and review the audit trail;

f) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools; and

g) recover to the state following the last backup.

F.AUDEVT The TOE generates an audit log of the following events:

a) Start-up and shutdown of the audit functions; and

b) All other remaining auditable events specified in Table 4.

F.AUDINF For each audit event entry, the TOE records, where applicable, at least the following information:

a) Date and time of the event;

b) type of event;

c) subjects’ identities;

d) outcome (success or failure) of the event; and

e) for each audit event type, based on the auditable event definitions of the functional components included in the ST, the information specified in column four of Table 4.

F.AUDRPT

The TOE provides a means for the authorized administrator to read all audit data in a manner that permits interpretation, and allows the administrator to perform searching and ordering of the audit data using the following categories:

a) presumed subject address;

b) ranges of dates;

c) ranges of times; and

d) ranges of addresses.

F.AUDSTO

The TOE protects audit data from unauthorized modification or deletion. The TOE prevents audit data loss by preventing auditable events, except those taken by the authorized administrator, when the audit trail is full and limits the number of audit records lost if the audit trail is full by managing log file size and location.

F.FWRULES

The TOE uses a security policy to restrict the ability of unauthenticated external IT entities to pass information to one another through the TOE. This security policy is based on at least the following types of subject and information security attributes:

a) subject security attributes:

i) presumed address;

b) information security attributes:

i) presumed address of source subject;
ii) presumed address of destination subject;
iii) transport layer protocol;
iv) TOE interface on which traffic arrives and departs;
v) service; and
vi) schedule, defined by days of the week and start/stop time.

F.FWINVOKED

The TOE ensures that all information flows provided to the TOE by external entities for transfer to other entities are subjected to the defined security policies and conform to them before they are allowed to proceed toward the destination entity. The policies are instantiated as firewall rules using the security attributes set by F.ADMIN before conformance is tested.

F.ADMIN

Access to the TOE is restricted to authorised administrators, and, if the management console is connected via Ethernet, is enforced upon an acceptable IP address. Each administrator has a set of privileges consistent with F.HMI which only allow the administrators to perform those tasks associated with their duties. One of the tasks that is restricted to the authorized administrator is to read, modify, delete or change the default values for the security attributes, defined in FDP_IFF.1.

| | |
|---|---|
| F.I&A | The TOE requires each user to identify itself and be successfully authenticated before allowing any other TOE-mediated actions on behalf of that user. Restrictions on acceptable passwords ensure that the probability that authentication data can be guessed is no greater than one in one million (0.000001). |
| F.DOMAIN | The TOE maintains an isolated security domain, within its enclosure, for its own execution that protects it from interference and tampering by untrusted subjects. Users cannot access the operating system. No general-purpose software runs on the system. It enforces separation between the security domains of subjects in the TSC by assigning each to a physical and logical input/output interface and by segregating and protecting security-critical data in a configuration file. |
| F.INIT | The TOE provides restrictive default values for information flow security attributes that are used to enforce the SFP, and allows the administrator to override the default values when an object or information is created. |
| F.NORESID | The TOE ensures that no information from previously processed information flows is transferred to subsequent information flows. This applies both to information that is input to the TOE from an external source and to information (e.g., padding bits) that might be added by the TOE during processing of the information from the external source. |
| F.TIME | The TOE provides reliable time stamps for its own use. |

## 6.2 ASSURANCE MEASURES

A description of each of the TOE assurance measures follows.

| | |
|---|---|
| M.ID | The TOE incorporates a unique version identifier that can be displayed to the user. |
| M.CMSYS | The TOE was developed and is maintained using a documented CM system, with automated support, to ensure that only authorised changes are made to the TOE configuration items and implemented in the evaluated version of the TOE and to support the generation of the TOE. The organization, operation and usage of the CM system are described in a CM plan, which describes the method used to uniquely identify the configuration items, describes the automated tools and their usage in the system, and identifies CM records that are to be retained as evidence that the CM system is operating in accordance with the plan and that all configuration items have been and are being effectively maintained under the CM system. A list that uniquely identifies and describes all configuration items that comprise the TOE, all TOE documentation, all configuration items required to create the TOE (i.e., implementation |

representation), security flaws and the evaluation evidence required by the assurance components of the ST, is maintained. The procedures used to accept modified or newly created configuration items as part of the TOE are documented in an acceptance plan.

M.GETTOE The developer uses a documented and controlled process and procedures for shipping a packaged TOE, identified by serial number, to a customer. The delivery documentation describes all procedures and technical measures that are necessary to maintain security and detect modifications or any discrepancy between the developer's master copy and the version received at the user site. The documentation describes how the procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

M.SETUP Documented procedures describe all the steps necessary for the secure installation, generation, and start-up of the TOE. Application of these procedures to the TOE results in a secure configuration.

M.SPEC The development documentation consists of a functional specification, a high level TOE design, and a low level TOE design.

The informal, internally consistent, functional specification describes the TSF and the purpose and method of use of all external TSF external interfaces, providing complete details of all effects, exceptions and error messages. The functional specification completely represents the TSF and includes rationale that the TSF is completely represented.

The informal, internally consistent high-level design describes the structure of the TSF in terms of TSP-enforcing and other subsystems, and, for each subsystem, describes the security functionality that it provides. The high-level design identifies all underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software. The high-level design identifies all interfaces to the subsystems of the TSF and identifies which of these interfaces are externally visible. The high-level design describes the purpose and method of use all interfaces to the subsystems of the TSF, and provides details of effects, exceptions and error messages, as appropriate.

The informal, internally consistent, low-level design describes the TSF in terms of TSP-enforcing and other modules, describes the purpose of each module, defines the interrelationships between the modules in terms of security functionality provided and dependencies on other modules, and describes how each TSP-enforcing function is provided. The low-level design identifies all interfaces to the modules of the TSF, identifies which of these interfaces are externally visible, and describes the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

M.IMPREP An internally consistent implementation representation unambiguously defines the TSF to a level of detail such that the TSF can be generated without further design decisions.

M.TRACE Correspondence mappings demonstrate that the security functionality detailed in the TOE functional specification is upwards traceable to this ST, downwards traceable to the high level design, low level design, implementation representation, and is traceable to the TSP model. For each adjacent pair of provided TSF representations, a correspondence analysis demonstrates that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

M.TOESPM The informal TOE security policy model describes the rules and characteristics of all policies of the TSP that can be modeled. The rationale included with the model demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled. Correspondence between the functional specification and the TSP model shows that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

M.DOCS Documentation is provided in the form of operational guidance for the administrator and for the user.

The administrator guidance describes the administrative functions and interfaces available to the administrator of the TOE, describes how to administer the TOE in a secure manner, and contains warnings about functions and privileges that should be controlled in a secure processing environment. The administrator guidance describes all assumptions regarding user behaviour that are relevant to secure operation of the TOE, describes all security parameters under the control of the administrator, indicating secure values as appropriate, and describes each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. The administrator guidance is consistent with all other documentation supplied for evaluation, and describes all security requirements for the IT environment that are relevant to the administrator. Procedurally, the administrator is required to choose a password with the following characteristics:

- One (or more) of the characters should be capitalized
- One (or more) of the characters should be numeric
- One (or more) of the characters should be non alpha-numeric (e.g. punctuation mark)

The user guidance describes the functions and interfaces available to the non-administrative users of the TOE, describes the use of user-accessible security functions provided by the TOE, and contains warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. The user guidance clearly presents all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment. The user guidance is consistent with all other documentation supplied for evaluation, and describes all security requirements for the IT environment that are relevant to the user. Flaw remediation guidance is provided to describe how TOE users report to the developer any suspected security flaws in the TOE. The flaw remediation guidance also describes a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections. The flaw remediation guidance identifies the specific points of contact for all reports and enquiries about security issues involving the TOE.

M.DEVSEC The development security documentation describes all the physical, procedural, personnel and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment and provides evidence that these security measures are followed during the development and maintenance of the TOE.

M.FLAWREM Flaw remediation procedures, addressed to TOE developers, establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to these flaws. The flaw remediation procedures documentation describes the procedures used to track all reported security flaws in each release of the TOE. The flaw remediation procedure requires that a description of the nature and effect of each flaw be provided, as well as the status of finding a correction to that flaw. The flaw remediation procedure requires that corrective actions be identified for each of the security flaws and the flaw remediation procedures documentation describes the methods used to provide flaw information, corrections, and guidance on corrective actions to TOE users. The flaw remediation procedures documentation describes a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE. The procedures for processing reported security flaws ensures that any reported flaws are corrected and the correction issued to TOE users. The procedures for processing reported security flaws provide safeguards that any corrections to these security flaws do not introduce any new flaws. The flaw remediation procedures include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

M.LIFECYCLE A life-cycle model has been established for use in the development and maintenance of the TOE. Life-cycle definition documentation has been produced that describes this life-cycle model. The life-cycle model provides for the necessary control over the development and maintenance of the TOE.

M.DEVTOOLS The development tools being used for the TOE have been identified and the selected implementation-dependent options of the development tools have been documented. All development tools used for implementation are well-defined. The documentation of the development tools unambiguously defines the meaning of all statements and of all implementation-dependent options used in the implementation.

M.TESTCOV An analysis of the test coverage demonstrates the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. This analysis demonstrates that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

M.TESTDPT An analysis of the depth of testing demonstrates that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

M.DEVTEST A suitably configured TOE is tested by the developer in a controlled environment to confirm that the TSF operates as specified, and that the TOE is protected from a representative set of well-known attacks. The developer-provided test documentation consists of test plans, test procedure descriptions, expected test results and actual test results. The test plans identify the security functions to be tested and describe the goal of the tests to be performed. The test procedure descriptions identify the tests to be performed and describe the scenarios for testing each security function. These scenarios include any ordering dependencies on the results of other tests. The expected test results show the anticipated outputs from a successful execution of the tests. The test results from the developer execution of the tests demonstrate that each tested security function behaved as specified.

M.INDTEST Independent tests, which are conducted on a suitable TOE, with the aid of a set of resources equivalent to those that were used in the developer's functional testing of the TSF, confirm that the TOE operates as specified.

M.VALIDANAL The guidance documentation identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation, lists all assumptions about the intended environment, and lists all requirements for external security measures (including external procedural, physical and personnel controls). This guidance documentation is complete, clear, consistent and reasonable. The fact that the guidance documentation provides sufficient information to permit the TOE to be configured and used securely using only the supplied guidance documentation, and allows all insecure states to be detected is confirmed by independent evaluation and performance of the procedures using only the supplied guidance. The developer-provided analysis of the guidance documentation demonstrates that the guidance documentation is complete, and that guidance is provided for secure operation in all modes of operation of the TOE.

M.SOFASS A strength of TOE security function analysis is performed and documented for F.I&A, which is the only mechanism identified in the ST as having a strength of TOE security function claim. This analysis shows that M.I&A meets or exceeds the specific strength of function metric defined in the ST.

M.VULANAL The TOE design is examined to ensure that the security functions adequately address perceived threats in the security environment. Threats include deliberate attempts to disable, bypass, and brute-force attack the TSF. A documented vulnerability analysis of the TOE deliverables is conducted in order to search for ways in which a user can violate the TSP, and the disposition of identified vulnerabilities is documented, showing, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. The vulnerability analysis documentation justifies that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks performed by an attacker possessing a low attack potential.

# 7 PROTECTION PROFILE CLAIMS

This section provides the TFFWLR PP conformance claim statements.

## 7.1 TFFWLR PP REFERENCE

The TOE conforms to the following TFFWLR PP:

- U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1 (Final), April 1999.

## 7.2 TFFWLR PP TAILORING

The following tailoring was applied to the TFFWLR PP to produce this ST:

- Requirements applicable only to remote administration, which is optional in this TFFWLR PP and is not supported by the TOE, were either marked deleted, if they impacted only part of a requirement, or removed entirely if the whole requirement ceased to be applicable.
- Requirements that requested ST author input were completed in accordance with the direction in the TFFWLR PP.
- The EAL2 assurance requirements of the TFFWLR PP were removed.
- The selection in FIA_UAU.1.1 was refined to "user identification as stated in FIA_UID.2" for consistency with FIA_UID.2, which deals with user identification.
- The definition of the TOE Security Functional Policy was amended to reference the TOE interfaces, which are under control of the TOE, instead of the external IT entities, which are not under control of the TOE.
- The assumption A.LOWEXP and related objective O.LOWEXP have been changed to A.HIGHEXP and O.HIGHEXP respectively to reflect the reasonable assumption that the TOE will be deployed between the Internet (i.e., the external network) and an organization's internal network.
- The objective O.REMACC has been deleted because remote administrative access is not supported.
- Non-applicable rows O.SINUSE and O.ENCRYP as well as non-applicable column T.PROCOM were removed from mapping Table 6.
- Non-applicable columns O.SINUSE and O.ENCRYP were removed from mapping Table 8.

As this tailoring impacted significant sections of the TFFWLR PP, the complete contents of the TFFWLR PP have been restated within the ST for clarity. The TFFWLR PP requirements have been reordered to match the standard CC presentation by class and family.

The identifications used in the TFFWLR PP have been carried over into the ST, with one exception. The exception occurs in 4.2.1, where the security objectives for the environment have been assigned a consistent O.x nomenclature instead of the mixed O.x and A.x that appears in the TFFWLR PP.

Minor grammatical corrections have been made to text copied from the PP. These changes do not change the meaning of the text.

## 7.3 TFFWLR PP ADDITIONS

The objective O.NOREMACC was added to emphasize the fact that no remote administrative access support is provided by the TOE and to provide traceability for A.REMACC, which is present in the TFFWLR PP.

The EAL4 assurance requirements of the TFFWLR PP were added.

FIA_SOS.1 was added as the TOE enforces a minimum password length.

FMT_MSA.1 was added for completeness as it is a dependency of FMT_MSA.3.

FMT_SMF.1, was added to satisfy a dependency that did not exist when the TFFWLR PP was published.

In response to consumer demand, one assurance requirement, ALC_FLR.3 was added to provide additional life cycle assurance when flaws in the TOE are uncovered.

# 8 RATIONALE

## 8.1 SECURITY OBJECTIVES RATIONALE

### 8.1.1 TOE Security Objectives Rationale

Table 6 provides a bi-directional mapping of Security Objectives to Threats as specified in the TFFWLR PP, tailored to remove the rows and columns that are not applicable to the TOE. It shows that each of the threats is addressed by at least one of the objectives and that each of the objectives addresses at least one of the threats. It is followed by a discussion of how each threat is addressed by the corresponding Security Objective(s).

| | T.AUDFUL | T.REPEAT | T.REPLAY | T.ASPOOF | T.MEDIAT | T.OLDINF | T.AUDACC | T.SELPRO | T.NOAUTH |
|---|---|---|---|---|---|---|---|---|---|
| O.IDAUTH | | X | | | | | | | X |
| O.MEDIAT | | | | X | X | X | | | |
| O.SECSTA | | | | | | | | X | X |
| O.SELPRO | X | | | | | | | X | |
| O.AUDREC | X | | | | | | X | | |
| O.ACCOUN | | | | | | | X | | |
| O.SECFUN | X | | X | | | | | X | X |
| O.LIMEXT | | | | | | | | X | X |

**Table 6 - Mapping of Security Objectives to Threats**

T.NOAUTH

*An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.*

O.IDAUTH - This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.

O.SECSTA This security objective ensures that no information is compromised by the TOE upon startup or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

O.LIMEXT This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.

T.REPEAT *An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.*

O.IDAUTH - This security objective is necessary to counter the threat: T.REPEAT because it requires that users be uniquely identified and authenticated before accessing the TOE.

T.REPLAY *An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.*

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

T.ASPOOF *An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network uses a spoofed source address.*

O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

T.MEDIAT *An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.*

O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

T.OLDINF *Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.*

O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

T.AUDACC *Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.*

O.AUDREC This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

T.SELPRO *An unauthorized person may read, modify, or destroy security critical TOE configuration data.*

O.SECSTA This security objective ensures that no information is compromised by the TOE upon startup or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.LIMEXT This security objective provides the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity, which prevents extension of privilege (e.g., unauthorized reading, modification, or destruction of security critical TOE configuration data), and thus contributes to countering threat T.SELPRO.

O.SECFUN This security objective ensures that only authorized administrators can use the TOE security functions, which contributes to countering T.SELPRO by not allowing unauthorized persons to read, modify or destroy security critical TOE configuration data.

T.AUDFUL *An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker’s actions.*

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

O.AUDREC This security objective requires the audit trail of security-related events to have accurate dates and times, which partially counters T.AUDFUL by making lost or missing audit records more evident.

### 8.1.2 Environment Security Objectives Rationale

Table 7 provides a bi-directional mapping of Security Objectives for the environment to Assumptions. It shows that each of the assumptions is addressed by at least one of the objectives and that each of the objectives addresses at least one of the assumptions. It is followed by a discussion of how each Assumption is addressed by the corresponding Security Objective(s).

| | A.PHYSEC | A.HIGHEXP | A.GENPUR | A.PUBLIC | A.NOEVIL | A.SINGEN | A.DIRECT | A.NOREMO | A.REMACC | T.TUSAGE | A.CONSOLE | A.CONSOLE_ACCESS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.PHYSEC | X | | | | | | | | | | | |
| O.HIGHEXP | | X | | | | | | | | | | |
| O.GENPUR | | | X | | | | | | | | | |
| O.PUBLIC | | | | X | | | | | | | | |
| O.NOEVIL | | | | | X | | | | | | | |
| O.SINGEN | | | | | | X | | | | | | |
| O.DIRECT | | | | | | | X | | | | | |
| O.NOREMO | | | | | | | | X | | | | |
| O.NOREMACC | | | | | | | | | X | | | |
| O.GUIDAN | | | | | | | | | | X | X | X |
| O.ADMTRA | | | | | | | | | | X | | |
| O.CONSOLE | | | | | | | | | | | X | |
| O.CONSOLE_ACCESS | | | | | | | | | | | | X |

**Table 7 - Mapping of Security Objectives to Assumptions**

A.PHYSEC *The TOE is physically secure.*

O.PHYSEC The TOE is physically secure.

A.HIGHEXP *The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered high.*

O.HIGHEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered high.

A.GENPUR *There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.*

O.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.PUBLIC *The TOE does not host public data.*

O.PUBLIC The TOE does not host public data.

A.NOEVIL *Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.*

O.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.SINGEN *Information can not flow among the internal and external networks unless it passes through the TOE.*

O.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

A.DIRECT *Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.*

O.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

A.NOREMO *Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.*

O.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

A.REMACC *Authorized administrators may access the TOE remotely from the internal and external networks.*

O.NOREMACC Authorized administrators are not able to access the TOE remotely from the internal and external networks.

| | |
|---|---|
| T.USAGE | *The TOE may be inadvertently delivered, configured, used and administered in an insecure manner by either authorized or unauthorized persons.* |
| | O.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security. |
| | O.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices. |
| A.CONSOLE | *A management console, configured in accordance with the administrative guidance, is directly connected to the TOE via a dedicated link entirely within a controlled area of the environment. The console is in the same physical location as the TOE and is physically secure. The console is expected to correctly transmit the information entered on it to the TOE; and to correctly display the information sent to it by the TOE.* |
| | O.CONSOLE A management console, configured in accordance with the administrative guidance, is directly connected to the TOE via a dedicated link entirely within a controlled area of the environment. The console is in the same physical location as the TOE and is physically secure. The console is expected to correctly transmit the information entered on it to the TOE and to correctly display the information sent to it by the TOE. |
| | O.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security. |
| A.CONSOLE_ACCESS | *Access to the console will be restricted to authorized administrators.* |
| | O.CONSOLE_ACCESS Access to the console will be restricted to authorized administrators. |
| | O.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security. |

## 8.2 SECURITY REQUIREMENTS RATIONALE

### 8.2.1 Security Functional Requirements Rationale

Table 8 provides a bi-directional mapping of Security Functional Requirements to Security Objectives. It shows that each of the applicable objectives for the TOE is addressed by at least one of the functions and that each of the functions addresses at least one of the objectives. The table is followed by a discussion of how each Security Objective is addressed by the corresponding Security Functional Requirements.

| | O.IDAUTH | O.MEDIAT | O.SECSTA | O.SELPRO | O.AUDREC | O.ACCOUN | O.SECFUN | O.LIMEXT |
|---|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | | | | | X | X | | |
| FAU_SAR.1 | | | | | X | | | |
| FAU_SAR.3 | | | | | X | | | |
| FAU_STG.1 | | | | X | | | X | |
| FAU_STG.4 | | | | X | | | X | |
| FDP_IFC.1 | | X | | | | | | |
| FDP_IFF.1 | | X | | | | | | |
| FDP_RIP.1 | | X | | | | | | |
| FIA_ATD.1 | X | | | | | X | | |
| FIA_SOS.1 | X | | | | | | | |
| FIA_UAU.1 | X | | | | | | | |
| FIA_UID.2 | X | | | | | | | |
| FMT_MOF.1 | | | X | | | | X | X |
| FMT_MSA.1 | X | | | | | | X | |
| FMT_MSA.3 | | X | X | | | | X | |
| FMT_SMF.1 | | | | | | | X | X |
| FMT_SMR.1 | | | | | | | X | |
| FPT_RVM.1 | | | | X | | | | |
| FPT_SEP.1 | | | | X | | | | |
| FPT_STM.1 | | | | | X | | | |

**Table 8 - Mapping of Security Functional Requirements to TOE Security Objectives**

FAU_GEN.1 Audit data generation

This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review

This component ensures that a variety of searches and sorts can be performed on the audit trail. As no pre-defined tools for searching and sorting have been defined, there is no constraint on the means by which TOE developers meet this requirement . This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

This component ensures that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. All audit data that has been stored either in memory or the hard disk can be expected to be lost in the event of audit storage failure, exhaustion and/or attack. This TOE mitigates this potential loss by generating warning log entries when the disk or memory allocated for logging is filled to 75%, then 90% and finally 95% of capacity. At 95% of capacity the default action is to block further traffic and switch to error mode. FAU_STG.4 traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FDP_IFC.1 Subset information flow control

This component identifies the entities involved in the UNAUTHENTICATED SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes

This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_RIP.1 Subset residual information protection

This component ensures that neither information that flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FIA_ATD.1 User attribute definition

This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH, and O.ACCOUN. For O.IDAUTH, these attributes enable identification and authentication to be performed. For O.ACCOUN, these attributes enable the users to be identified, for later association with auditable actions, thus aiding in providing accountability.

FIA_SOS.1 Specification of secrets

This component ensures that there are defined quality metrics on the authentication data. This component traces back to and aids in meeting the following objective: O.IDAUTH.

FIA_UAU.1 Timing of authentication

This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. An additional SOF metric for this requirement is defined in section 5.1.1 to ensure that the authentication mechanism chosen cannot be easily bypassed. This component traces back to and aids in meeting the O.IDAUTH objective.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the objective O.IDAUTH.

FMT_MOF.1 Management of security functions behavior

This component consolidates all TOE management/administration/security functions. It traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA. It has been modified via permitted CC operations.

FMT_MSA.1 Management of security attributes

This component ensures that the ability to change_default, delete, modify, and read security attributes is limited to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.

FMT_MSA.3 Static attribute initialization

This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT , O.SECSTA, and O.SECFUN.

FMT_SMF.1 Specification of Management Functions

This component ensures that the TOE can actually perform the required security management functions. It traces back to and aids in meeting the following objectives: O.SECFUN and O.LIMEXT. It complements FMT_MOF.1, which restricts the performance of these functions.

FMT_SMR.1 Security roles

Each of the CC class FMT components in this Security Target depends on this component for the specified roles. This component traces back to and aids in meeting the following objective: O.SECFUN.

FPT_RVM.1 Non-bypassability of the TSP

This component ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_SEP.1 TSF domain separation

This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

### 8.2.2 Assurance Requirements Rationale

For business competitive reasons, Fortinet has decided that the TOE be evaluated at EAL4, augmented with flaw remediation. This combination is termed EAL4+. This provides a level of independently assured security that is higher than the level specified by the TFFWLR PP, and is therefore consistent with the postulated threat environment, which was taken from the TFFWLR PP. Specifically, the threat of malicious attacks is not greater than moderate, and the product has undergone a search for obvious flaws. Specification of EAL4+ includes the vulnerability assessment component AVA_VLA.2, Independent vulnerability analysis, which aids in providing assurance that the product will be able to cope with some of the malicious attacks implied by attackers possessing low attack potential.

### 8.2.3 Rationale for Satisfying Functional Requirement Dependencies

Table 9 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency.

| Security Functional Requirement | Dependencies | Dependency Satisfied | Notes |
|---|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | Yes | |
| FAU_SAR.1 | FAU_GEN.1 | Yes | |
| FAU_SAR.3 | FAU_SAR.1 | Yes | |
| FAU_STG.1 | FAU_GEN.1 | Yes | |
| FAU_STG.4 | FAU_STG.1 | Yes | |
| FDP_IFC.1 | FDP_IFF.1 | Yes | |
| FDP_IFF.1 | FDP_IFC.1<br>FMT_MSA.3 | Yes | |
| FDP_RIP.1 | None | N/A | |
| FIA_ATD.1 | None | N/A | |
| FIA_SOS.1 | None | N/A | |
| FIA_UAU.1 | FIA_UID.1 | Yes | FIA_UID.2 is hierarchial |
| FIA_UID.2 | None | N/A | |
| FMT_MOF.1 | FMT_SMF.1[17]<br>FMT_SMR.1 | Yes<br>Yes | |
| FMT_MSA.1 | [FDP_ACC.1 or FDP_IFC.1]<br>FMT_SMF.1<br>FMT_SMR.1 | [No or Yes]<br>Yes<br>Yes | |
| FMT_MSA.3 | FMT_MSA.1<br>FMT_SMR.1 | Yes<br>Yes | |
| FMT_SMF.1 | None | N/A | |
| FMT_SMR.1 | FIA_UID.1 | Yes | FIA_UID.2 is hierarchial |
| FPT_RVM.1 | None | N/A | |
| FPT_SEP.1 | None | N/A | |

[17] Added as a result of Interpretation 065.

| Security Functional Requirement | Dependencies | Dependency Satisfied | Notes |
|---|---|---|---|
| FPT_STM.1 | None | N/A | |

**Table 9 - Security Functional Requirement Dependencies**

### 8.2.4 Rationale for Satisfying Assurance Requirement Dependencies

Table 10 identifies the Security Assurance Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency.

| Security Assurance Requirement | Dependencies | Dependency Satisfied | Notes |
|---|---|---|---|
| ACM_AUT.1 | ACM_CAP.3 | Yes | ACM_CAP.4 is hierarchical |
| ACM_CAP.4 | ALC_DVS.1 | Yes | |
| ACM_SCP.2 | ACM_CAP.3 | Yes | ACM_CAP.4 is hierarchical |
| ADO_DEL.2 | ACM_CAP.3 | Yes | ACM_CAP.4 is hierarchical |
| ADO_IGS.1 | AGD_ADM.1 | Yes | |
| ADV_FSP.2 | ADV_RCR.1 | Yes | |
| ADV_HLD.2 | ADV_FSP.1<br>ADV_RCR.1 | Yes<br>Yes | ADV_FSP.2 is hierarchical |
| ADV_IMP.1 | ADV_LLD.1<br>ADV_RCR.1<br>ALC_TAT.1 | Yes<br>Yes<br>Yes | |
| ADV_LLD.1 | ADV_HLD.2<br>ADV_RCR.1 | Yes<br>Yes | |
| ADV_RCR.1 | None | N/A | |
| ADV_SPM.1 | ADV_FSP.1 | Yes | ADV_FSP.2 is hierarchical |
| AGD_ADM.1 | ADV_FSP.1 | Yes | ADV_FSP.2 is hierarchical |
| AGD_USR.1 | ADV_FSP.1 | Yes | ADV_FSP.2 is hierarchical |
| ALC_DVS.1 | None | N/A | |
| ALC_FLR.3 | None | N/A | |
| ALC_LCD.1 | None | N/A | |
| ALC_TAT.1 | ADV_IMP.1 | Yes | |
| ATE_COV.2 | ADV_FSP.1<br>ATE_FUN.1 | Yes<br>Yes | ADV_FSP.2 is hierarchical |

| Security Assurance Requirement | Dependencies | Dependency Satisfied | Notes |
|---|---|---|---|
| ATE_DPT.1 | ADV_HLD.1<br>ATE_FUN.1 | Yes<br>Yes | ADV_HLD.2 is hierarchical |
| ATE_FUN.1 | None | N/A | |
| ATE_IND.2 | ADV_FSP.1<br>AGD_ADM.1<br>AGD_USR.1<br>ATE_FUN.1 | Yes<br>Yes<br>Yes<br>Yes | ADV_FSP.2 is hierarchical |
| AVA_MSU.2 | ADO_IGS.1<br>ADV_FSP.1<br>AGD_ADM.1<br>AGD_USR.1 | Yes<br>Yes<br>Yes<br>Yes | ADV_FSP.2 is hierarchical |
| AVA_SOF.1 | ADV_FSP.1<br>ADV_HLD.1 | Yes<br>Yes | ADV_FSP.2 is hierarchical<br>ADV_HLD.2 is hierarchical |
| AVA_VLA.2 | ADV_FSP.1<br>ADV_HLD.2<br>ADV_IMP.1<br>ADV_LLD.1<br>AGD_ADM.1<br>AGD_USR.1 | Yes<br>Yes<br>Yes<br>Yes<br>Yes<br>Yes | ADV_FSP.2 is hierarchical |

**Table 10 - Security Assurance Requirement Dependencies**

### 8.2.5 Rationale for Security Functional Refinements

FAU_GEN.1 Audit data generation

The refinement “relevant” has been added to FAU_GEN.1.1b to match the TFFWLR PP.

The term “subject identity” in FAU_GEN.1.2a has been changed to “subjects’ identities” to match the TFFWLR PP.

FDP_IFF.1 Simple security attributes

The refinement “at least” has been added to FDP_IFF.1.1 to match the TFFWLR PP.

The wording of the main text of FDP_IFF.1.2 has been modified to match the TFFWLR PP.

FMT_MOF.1 Management of security functions behaviour

The selection in the body of FMT_MOF.1.1 has been extended to include the TFFWLR PP term “perform”. In accordance with Interpretation 065, this section restricts the performance of the functions to the authorized administrator, while FMT_SMF specifies the management functions that are actually provided. Functions related to remote administration were deleted as the TOE does not provide any support for remote administration.

FMT_MSA.3

The refinement “information flow” to security attributes in FMT_MSA.3.1 is added to match the TFFWLR PP.

FMT_SMR.1 Security roles

The word “roles” has been changed to “role” in FMT_SMR.1.1 to match the singular form of “authorized administrator”.

In FMT_SMR.1.2, the refinement “human” is added to match the TFFWLR PP. The article “the” has been inserted to improve the flow of the sentence.

### 8.2.6 Rationale for Audit Exclusions

The auditable events associated with FIA_AFL.1 in the TFFWLR PP have been excluded because remote administration has been excluded, so there is nothing to audit.

The auditable events associated with FCS_COP.1 in the TFFWLR PP have been excluded because this function has been excluded from this ST.

## 8.3 EXPLICITLY STATED REQUIREMENTS RATIONALE

As this ST does not contain any explicitly stated requirements, this section is not applicable.

## 8.4 TOE SUMMARY SPECIFICATION RATIONALE

### 8.4.1 TOE Security Functions Rationale

Table 11 provides a bi-directional mapping of Security Functions to Security Functional Requirements. It shows that each of the SFRs is addressed by at least one of the Security Functions and that each of the Security Functions addresses at least one of the SFRs. The table is followed by a discussion of how each Security Functional Requirement is addressed by the corresponding Security Function.

| | FAU_GEN.1 | FAU_SAR.1 | FAU.SAR.3 | FAU_STG.1 | FAU_STG.4 | FDP_IFC.1 | FDP_IFF.1 | FDP_RIP.1 | FIA_ATD.1 | FIA_SOS.1 | FIA_UAU.1 | FIA_UID.2 | FMT_MOF.1 | FMT_MSA.1 | FMT_MSA.3 | FMT_SMF.1 | FMT_SMR.1 | FPT_RVM.1 | FPT_SEP.1 | FPT_STM.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| F.HMI | | | | | | | | | X | | | | X | X | | X | X | | | |
| F.AUDEVT | X | | | | | | | | | | | | | | | | | | | |
| F.AUDINF | X | | | | | | | | | | | | | | | | | | | X |
| F.AUDRPT | | X | X | | | | | | | | | | | | | | | | | |

| | FAU_GEN.1 | FAU_SAR.1 | FAU.SAR.3 | FAU_STG.1 | FAU_STG.4 | FDP_IFC.1 | FDP_IFF.1 | FDP_RIP.1 | FIA_ATD.1 | FIA_SOS.1 | FIA_UAU.1 | FIA_UID.2 | FMT_MOF.1 | FMT_MSA.1 | FMT_MSA.3 | FMT_SMF.1 | FMT_SMR.1 | FPT_RVM.1 | FPT_SEP.1 | FPT_STM.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| F.AUDSTO | | | | X | X | | | | | | | | | | | | | | | |
| F.FWRULES | | | | | | X | X | | | | | | | | | | | | | |
| F.FWINVOKED | | | | | | | X | | | | | | | | | | | X | | |
| F.ADMIN | | | | | | | | | X | | | | | X | | | X | | | |
| F.I&A | | | | | | | | | | X | X | X | | | | | | | | |
| F.DOMAIN | | | | | | | | | | | | | | | | | | | X | |
| F.INIT | | | | | | | | | | | | | | | X | | | | | |
| F.NORESID | | | | | | | | X | | | | | | | | | | | | |
| F.TIME | X | | | | | | | | | | | | | | | | | | | X |

**Table 11 - Mapping of Security Functions to Security Functional Requirements**

FAU_GEN.1 Audit data generation

F.AUDEVT, F.AUDINF and F.TIME combine to satisfy the requirement for the generation of audit data for the specified set of TOE events. F.AUDEVT generates an appropriate log, F.AUDINF provides appropriate entries, and F.TIME provides a reliable time stamp for the entries.

FAU_SAR.1 Audit review

F.AUDRPT satisfies the requirement to provide audit data to the authorized administrator in a manner that permits interpretation.

FAU_SAR.3 Selectable audit review

F.AUDRPT satisfies the requirement to allow selectable reviewing of audit data by searching and ordering the data based on defined categories.

FAU_STG.1 Protected audit trail storage

F.AUDSTO satisfies the requirement for protected storage of audit data by managing log file size and location.

FAU_STG.4 Prevention of audit data loss

F.AUDSTO satisfies the requirement to protect stored audit data and to minimize data loss if the audit trail is full.

FDP_IFC.1 Subset information flow control

F.FWRULES satisfies the requirement to enforce security policy on entities that send and information through the TOE to one another.

FDP_IFF.1 Simple security attributes

F.FWRULES and F.FWINVOKED combine to satisfy the requirement for security policy enforcement based on subject security attributes and on information security attributes. F.FWINVOKED ensures that all information flows are subjected to the firewall policy. F.FWRULES satisfies the requirement for a configurable mechanism.

FDP_RIP.1 Subset residual information protection

F.NORESID satisfies the requirement to ensure that the information content of a resource is not made available when the resource is allocated to another object for subsequent processing. This applies to information that originates in the TOE as well as to information that originated in the external source.

FIA_ATD.1 User attribute definition

F.ADMIN satisfies the requirement to maintain a list of security attributes belonging to individual users. F.HMI provides the interface through which the attributes are modified.

FIA_SOS.1

F.I&A satisfies the requirement to authenticate the administrator and ensures that the specific strength of function metrics are met.

FIA_UAU.1 Timing of authentication

F.I&A satisfies the requirement to allow identification of the administrator before authentication and to require authentication before allowing any other TSF-mediated actions on behalf of that administrator.

FIA_UID.2 User identification before any action

F.I&A satisfies the requirement for each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FMT_MOF.1 Management of security functions behavior

F.HMI satisfies the requirement for the TOE to provide the user with the capability to manage the security functions of the TOE through external interfaces.

FMT_MSA.1 Management of security attributes

F.ADMIN satisfies the requirement to restrict the ability to manage (i.e., change_default, delete, modify, read) the security attributes to the authorized administrator. F.HMI provides the authorized administrator with the ability to manage these security attributes.

FMT_MSA.3 Static attribute initialization

F.INIT satisfies the requirement for the default TOE configuration.

FMT_SMF.1 Specification of Management Functions

F.HMI satisfies the requirement to manage the TOE security management functions.

FMT_SMR.1 Security roles

F.ADMIN satisfies the requirement for a security administration role and F.HMI satisfies the requirement for the TOE to provide the administrator with the capability to manage the security attributes of the TOE.

FPT_RVM.1 Non-bypassability of the TSP

F.FWINVOKED satisfies the requirement for the TOE to ensure that the enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF domain separation

F.DOMAIN satisfies the requirement for the TOE to maintain a protected security domain for its own execution and to enforce separation between the security domains within its scope of control.

FPT_STM.1 Reliable time stamps

F.AUDINF and F.TIME combine to satisfy the requirement for the TOE to provide a reliable time and date for the time stamping of audit log entries.

### 8.4.2 TOE Assurance Measures Rationale

Table 12 provides a bi-directional mapping of Assurance Measures to Assurance Requirements. It shows that each of the Assurance Requirements is addressed by at least one of the Assurance Measures and that each of the Assurance Measures addresses at least one of the Assurance Requirements. The table is followed by a short discussion of how the Assurance Requirement are addressed by the corresponding Assurance Measures.

| | ACM_AUT.1 | ACM_CAP.4 | ACM_SCP.2 | ADO_DEL.2 | ADO_IGS.1 | ADV_FSP.2 | ADV_HLD.2 | ADV_IMP.1 | ADV_LLD.1 | ADV_RCR.1 | ADV_SPM.1 | AGD_ADM.1 | AGD_USR.1 | ALC_DVS.1 | ALC_FLR.3 | ALC_LCD.1 | ALC_TAT.1 | ATE_COV.2 | ATE_DPT.1 | ATE_FUN.1 | ATE_IND.2 | AVA_MSU.2 | AVA_SOF.1 | AVA_VLA.2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M.ID | | X | | | | | | | | | | | | | | | | | | | | | | |
| M.CMSYS | X | X | X | | | | | | | | | | | | | | | | | | | | | |
| M.GETTOE | | | | X | | | | | | | | | | | | | | | | | | | | |
| M.SETUP | | | | | X | | | | | | | | | | | | | | | | | | | |
| M.SPEC | | | | | | X | X | | X | | | | | | | | | | | | | | | |
| M.IMPREP | | | | | | | | X | | | | | | | | | | | | | | | | |
| M.TRACE | | | | | | | | | | X | | | | | | | | | | | | | | |
| M.TOESPM | | | | | | | | | | | X | | | | | | | | | | | | | |
| M.DOCS | | | | | | | | | | | | X | X | | X | | | | | | | | | |
| M.DEVSEC | | | | | | | | | | | | | | X | | | | | | | | | | |
| M.FLAWREM | | | X | | | | | | | | | | | | X | | | | | | | | | |
| M.LIFECYCLE | | | | | | | | | | | | | | | | X | | | | | | | | |
| M.DEVTOOLS | | | | | | | | | | | | | | | | | X | | | | | | | |
| M.TESTCOV | | | | | | | | | | | | | | | | | | X | | | | | | |
| M.TESTDPT | | | | | | | | | | | | | | | | | | | X | | | | | |
| M.DEVTEST | | | | | | | | | | | | | | | | | | | | X | | | | |
| M.INDTEST | | | | | | | | | | | | | | | | | | | | | X | | | |
| M.VALIDANAL | | | | | | | | | | | | | | | | | | | | | | X | | |
| M.SOFASS | | | | | | | | | | | | | | | | | | | | | | | X | |
| M.VULANAL | | | | | | | | | | | | | | | | | | | | | | | | X |

**Table 12 - Mapping of Assurance Measures to Assurance Requirements**

ACM_AUT.1 Partial CM automation

M.CMSYS satisfies the requirement for a CM system with automation support for change control and for TOE generation.

ACM_CAP.4 Generation support and acceptance procedures

M.ID and M.CMSYS combine to satisfy the requirement for a CM system that supports controlled generation of the TOE and acceptance of new or changed configuration items into the TOE.

ACM_SCP.2 Problem tracking CM coverage

M.CMSYS and M.FLAWREM combine to satisfy the requirement for controlling security flaws and tracking them to their resolution.

ADO_DEL.2 Detection of modification

M.GETTOE satisfies the requirement for defined delivery procedures with the ability to detect modifications to the TOE while in transit.

ADO_IGS.1 Installation, generation, and start-up procedures

M.SETUP satisfies the requirement for installation, generation and start-up procedures.

ADV_FSP.2 Fully defined external interfaces

M.SPEC satisfies the requirement for a functional specification with fully defined external interfaces.

ADV_HLD.2 Security enforcing high-level design

M.SPEC satisfies the requirement for a security enforcing high-level design.

ADV_IMP.1 Subset of the implementation of the TSF

M.IMPREP satisfies the requirement to provide a subset of the implementation of the TSF for review.

ADV_LLD.1 Descriptive low-level design

M.SPEC satisfies the requirement for a descriptive low-level design.

ADV_RCR.1 Informal correspondence demonstration

M.TRACE satisfies the requirement to informally demonstrate that more abstract TSF representations are correctly and completely refined into less abstract TSF representations.

ADV_SPM.1 Informal TOE security policy model

M.TOESPM satisfies the requirement for a model of the TSP.

AGD_ADM.1 Administrator guidance

M.DOCS satisfies the requirement for administrator guidance documentation.

AGD_USR.1 User guidance

M.DOCS satisfies the requirement for user guidance documentation.

ALC_DVS.1 Identification of security measures

M.DEVSEC satisfies the requirement to identify and documental developmental security measures.

ALC_FLR.3 Systematic flaw remediation

M.FLAWREM satisfies the requirement for systematically accepting and remediating security flaws. M.DOCS provides the documentation required to enable users to interact with the developers to report flaws and obtain corrections.

ALC_LCD.1 Developer defined life-cycle model

M.LIFECYCLE satisfies the requirement to establish and document a life-cycle model for TOE development and maintenance.

ALC_TAT.1 Well-defined development tools

M.DEVTOOLS satisfies the requirement for identification and documentation of the development tools being used for the TOE.

ATE_COV.2 Analysis of coverage

M.TESTCOV satisfies the requirement to provide an analysis of test coverage.

ATE_DPT.1 Testing: high-level design

M.TESTDPT satisfies the requirement to provide an analysis of the depth of testing to demonstrate that the TSF operates in accordance with its high-level design.

ATE_FUN.1 Functional Testing

M.DEVTEST satisfies the requirement to test the TSF and document the results.

ATE_IND.2 Independent testing – sample

M.INDTEST satisfies the requirement to support independent testing of a selected sample of the developer tests.

AVA_MSU.2 Validation of analysis

M.VALIDANAL satisfies the requirement to document an analysis of the competeness of the guidance documentation.

AVA_SOF.1 Strength of TOE security function evaluation

M.SOFASS satisfies the requirement for evidence that all TOE security functions have been examined to ensure their strengths against threats.

AVA_VLA.2 Independent vulnerability analysis

M.VULANAL satisfies the requirement to perform and document a vulnerability analysis.

## 8.5 STRENGTH OF FUNCTION RATIONALE

FortiGate Antivirus Firewalls provide a level of protection that is appropriate against threat agents whose attack potential is low, in IT environments that require that information flows be controlled and restricted among network nodes where the FortiGate unit can be appropriately protected from physical attacks. The FortiGate unit's management console must be controlled to restrict access to only authorized administrators. It is expected that the FortiGate units will be protected to the extent necessary to ensure that they remain connected to the networks they protect. The minimum strength of function, SOF-Basic, which is specified by the TFFWLR PP, is consistent with those requirements.

The required strength of function metric for the probability that authentication data can be guessed was taken from the TFFWLR PP. The password rules will ensure that the implementation has the required strength.

## 8.6 TFFWLR PP CLAIMS RATIONALE

The objectives O.CONSOLE and O.CONSOLE_ACCESS define how administration is performed and are additional to the TFFWLR PP claims. These objectives were added since remote administration is not being claimed.

The component FMT_MSA.1 (Management of security attributes) was added for completeness in meeting all dependencies for FMT_MSA.3. The rationale given in the TFFWLR PP for omitting this SFR was felt to be inadequate. It traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.

# 9 ACRONYMS, ABBREVIATIONS, AND INITIALIZATIONS

| | |
|---|---|
| ASIC | Application-Specific Integrated Circuit |
| CC | Common Criteria |
| CLI | Command Line Interface |
| CM | Configuration Management |
| DMZ | Demilitarized Zone |
| EAL | Evaluation Assurance Level |
| FIPS | Federal Information Processing Standard |
| FTP | File Transfer Protocol |
| FW | Firewall |
| GUI | Graphical user interface |
| HMI | Human-Machine Interface |
| HTTP | HyperText Transfer Protocol |
| I&A | Identification and Authentication |
| I/O | Input/Output |
| ID | Identification |
| IMAP | Internet Message Access Protocol |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| IT | Information Technology |
| LCD | Liquid Crystal Display |
| NAT | Network Address Translation |
| POP3 | Post Office Protocol Version 3 |
| PP | Protection Profile |
| SFP | Security Functional Policy |
| SFR | Security Functional Requirement |
| SMTP | Simple Mail Transfer Protocol |
| SOF | Strength of Function |
| SOHO | Small Office or Home Office |
| ST | Security Target |
| TBD | To Be Determined |
| TCP | Transmission Control Protocol |

| | |
|---|---|
| TOE | Target of Evaluation |
| TP | Transparent (Mode) |
| TSC | TSF Scope of Control |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |
| URL | Uniform Resource Locator |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |