Security Target for

Astaro Security Gateway Software V6.300

CC Compliant Software

EAL 2+

September 04, 2006

Version 2.08

Prepared by:
Astaro AG,
Amalienbadstraße 36 Bau 33a,
76227 Karlsruhe,
Germany

TABLE OF CONTENTS

List of Tables

List of Figures

Revision History

Date	Version	Author	Changes
2006-01-06	1.12	Krummeck	Revision history, consistency of claims wrt. forbidden remote administration, description of PP tailoring in chapter 7
2006-01-22	1.13	Krummeck	Incorporation of developer comments Consistency of Rationale
2006-01-28	1.14	Krummeck	More developer comments, consistency of chapter 5 and 6, updates to rationale reflecting these changes; section 6.1 on ASG architecture added
2006-02-05	1.15	Semrau	All comments have been removed after checking. Revision and ST layout changes (Astaro Word Template)
2006-02-07	1.16	Semrau	Chapter 1.3: replacement “systematic” by “basic” flaw remediation.
2006-03-07	2.00	Semrau	Basis for PDF file to be delivered to the BSI
2006-03-08	2.01	Krummeck	Added security objectives for the environment mapping to environment SFRs, deleted environment TSF
2006-03-10	2.02	Krummeck	Fixed some references, updated revision history
2006-04-25	2.03	Semrau	Changed TOE Version to 6.202, updated revision history
2006-05-11	2.04	Krummeck	Added SAR rationale, new versions of RPM packages
2006-07-14	2.05	Krummeck	Changed TOE version to 6.300, updated RPM list in section 2.3
2006-07-18	2.06	Becker	Replaced TOE diagram in Chapter 6.1; added a phrase explaining the logical interface in Chapter 6.1.2; changed references to ASG Software V6.2 to V6.3.
2006-07-25	2.07	Becker	Refined FIA_SOS.1 requirements; replaced TOE diagram in Chapter 6.1; added section specifying logging components.
2006-09-04	2.08	Becker	Updated list of RPMs in Section 2.3; redefined NAT as not being security enforcing; removed typos (incorrect “astaro” spelling).

1 Introduction

1.1 Identification

This document is the Security Target (ST) for the Astaro Security Gateway Software firewall component, version 6.300, hereinafter referred to as "ASG Software".

Documentation for the ASG Software operating in Common Criteria mode consists of the standard ASG Software V6.3 documentation set plus a CC-specific technical note.

This ST has been prepared in accordance with the Common Criteria for Information Security Evaluation (CC), Version 2.3, August 2005, CCIMB-2005-08-001 - 003.

1.2 Overview

Astaro Security Gateway features, among other things, a firewall, virus, spam, and phishing protection solution.

The Astaro Security Gateway is either available as ASG Software (delivered as a CD package or by download from the Astaro website), or as a hardware unit called ASG Appliance, having ASG Software pre-installed.

The Target of Evaluation (TOE) consists of the two constituent ASG Software firewall components which manage data traffic between networks according to configurable rule-based procedures: the Packet Filter and NAT (Network Address Translation).

For the aforementioned features not included in the TOE see Section 2.1.2.

Currently, the following models of ASG Appliances running the ASG Software exist:

	Interfaces			
Unit	**Ethernet Ports**	**Console**	**Control Panel**	**USB[1]**
ASG 110	3x 10/100	1x RS-232	no	2
ASG 120	3x 10/100	1x RS-232	no	2
ASG 220	8x 10/100	2x RS-232	4 button LCD	2
ASG 320	4x 10/100/1000 4x 10/100	2x RS-232	4 button LCD	4
ASG 425	8x 10/100/1000	2x RS-232	4 button LCD	4

[1] USB Universal Serial Port

ASG-525	10x 10/100/1000 1x 10/100	2x RJ-45	4 button LCD	2
	Interfaces			
Unit	**Ethernet Ports**	**Console**	**Control Panel**	**USB[2]**
ASG-525F	4x 10/100/1000 + 6x Gigabit Ethernet SFP 1x 10/100	2x RJ-45	4 button LCD	2

Table 1: Astaro Security Gateway Appliances – Hardware Specification

Astaro Security Gateway is a unified threat management system. It is designed to protect computer networks from unauthorized access and abuse. Astaro Security Gateway resides between the network which it is protecting and an external network such as the Internet. It spans a wide range of network environments from the small and home office to large enterprises. Astaro Security Gateway detects and eliminates damaging, content-based threats from email and web traffic such as viruses, worms, intrusions, inappropriate web-content, and so on in real-time without degrading network-performance. Additionally, it provides a broad range of security features such as Virtual Private Network (VPN), intrusion detection and prevention, anti-virus capabilities, anti-spam capabilities, and URL filtering under one unified management platform. Due to its NAT/router capabilities Astaro Security Gateway is capable to apply security features between two or more different networks, for example, between the local network and the Internet.

A separate management console called *WebAdmin* is the web-based GUI administering Astaro Security Gateway.

Application Note: TOE access via *WebAdmin* is limited to users who have authenticated themselves against the TOE. They are hereinafter referred to as “administrators”.

1.3 CC Conformance

ASG Software is in conformity with the identified functional requirements specified in Part 2 of the CC. ASG Software also conforms to the assurance requirements for Evaluation Assurance Level (EAL) 2, as specified in Part 3 of the CC, with the following augmentation:

- ALC_FLR.1 – Basic Flaw Remediation

The Target of Evaluation (TOE) for this ST also conforms to the following Protection Profile (PP):

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

[2] USB Universal Serial Port

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 italicized, 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 struck out 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 conventions 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

ASG Software is a network security application which includes a firewall in order to control network access.

The firewall is used for perimeter security in which it controls the data transferred between two networks of which one is called to be “external” and the other one which is called “internal”. The internal network and its assets are also protected by the firewall from unauthorized access. ASG Software is also capable of controlling the data stream between multiple networks or segments.

Figure 1 shows a typical scenario in which ASG Software is deployed between an external and internal network.

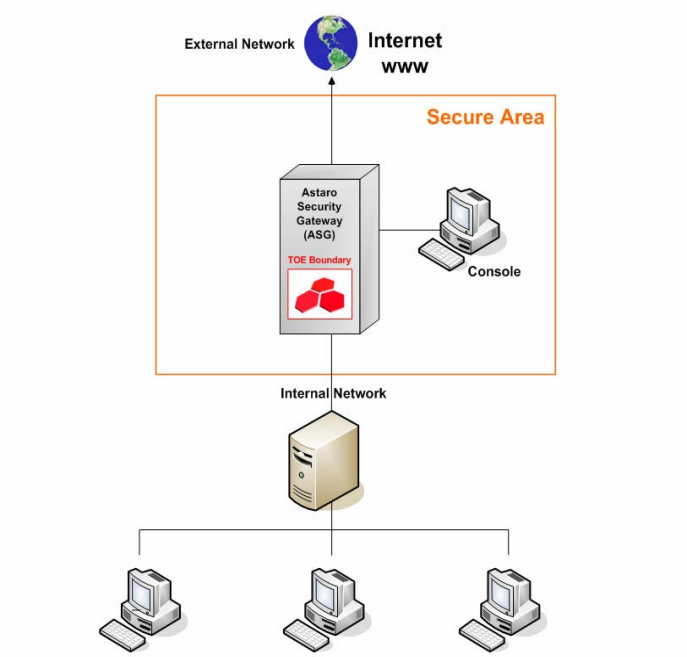

Figure 1 Typical ASG Network Configuration

The Target of Evaluation (TOE) consists of the two constituent ASG Software firewall components which manage data traffic between networks according to configurable rule-based procedures: the Packet Filter and NAT (Network Address Translation), whereas NAT is not a security enforcing function in the context of this evaluation.

The Packet Filter allows for selective passing or blocking of data packets as they pass through network interfaces.

Network Address Translation (NAT) provides for changing traffic source and destination parameters by hiding internal IP addresses.

For a picture of the ASG architecture and the relation of TOE to non-TOE components, see Figure 2 in section 6.1. ASG Software is designed to be installed and used in an environment which is configured and controlled in accordance with the administrator's guide that is shipped together with the software.

ASG software is administered from a console directly connected to the firewall within the secure area. No remote administration is anticipated.

2.1 Logical Description

2.1.1 Features Included in TOE

2.1.1.1 Access Control

ASG Software provides a role-based access control capability to ensure that only administrators are able to manage ASG Software.

2.1.1.2 Information Flow Control

ASG Software implements stateful inspection. Information flow is restricted by default but permitted by a set of rules that are defined by the administrator.

2.1.1.3 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.

2.1.1.4 Administration

On all gateways 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 GUI and allows an authorized administrator to configure ASG Software, monitor its operation, examine the audit logs that are created, and perform backup and archive activities.

Administration handling is provided by a separate user authentication daemon called AUA which operating system independently processes all authentication requests.

2.1.2 Features Excluded from TOE

Following features of ASG are outside the scope of the TOE and thus not evaluated. They are generally available but are required to be disabled in order to be compliant to a CC compatible configuration of the TOE.

2.1.2.1 VPN

ASG Software supports Virtual Private Networking (VPN) to provide a secure connection between widely separated office networks or securely link remote office employees or outside representatives to an office network.

2.1.2.2 Virus-Protection

ASG Software provides anti-virus protection for:

- Hypertext Transfer Protocol (HTTP),
- Simple Mail Transfer Protocol (SMTP),
- Post-Office Protocol Version 3 (POP3).

ASG Software can be configured in a way that virus pattern definitions are always up-to-date.

2.1.2.3 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.

2.1.2.4 Email Filtering

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

2.1.2.5 Reporting

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

2.1.2.6 Intrusion Prevention

ASG Software incorporates an Intrusion Prevention System (IPS) that detects and prevents suspicious network activities in real time. The IPS definitions can be updated manually or ASG Software can be configured to automatically download updates.

2.1.2.7 Spam-Protection

ASG Software provides Spam-Protection to detect and block unsolicited emails. It performs a series of tests and assigns a so-called “spam score” to each message indicating the probability that the message is unsolicited. Messages whose score exceeds certain thresholds set by the administrator will be dropped, returned to the sender, passed to the recipient with a warning, or quarantined.

2.1.2.8 Web proxy user authentication

ASG software provides the capability to restrict the usage of the HTTP, SMTP, or SOCKS proxies to users which have successfully identified and authenticated themselves to the firewall system.

2.1.2.9 Remote administration

ASG software can be configured to be administered from machines within one of the connected networks using additional security functions to ensure a secure administration. As these functions have not been part of the evaluation, only administration from locally connected consoles is permitted.

2.1.2.10 PPTP

The Point-to-Point Tunneling Protocol (PPTP) has not been subject of this evaluation and cannot be used in the TOE's evaluated configuration.

2.1.3 Features Not Supported

ASG Software provides a high-availability capability providing a failover mechanism between two or more appliances. As the TOE consists of one ASG Software instance only, this feature is not supported in the configuration to be evaluated.

2.2 TOE Security Functional Policies

This ST includes a single information flow control Security Function Policy (SFP). The information flow control SFP is called the UNAUTHENTICATED SFP. The subjects under control of this policy are 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 each information flow control SFP are found in FDP_IFF.1.2. The security functional requirement FMT_MSA.3 demands that these rules be assigned restrictive initial values. FMT_MSA.1 ensures that the rules are subsequently managed only by the authorized administrator.

2.3 TOE Boundary

The TOE software runs on top of a Linux operating system, which is delivered with the ASG product, but considered to be part of the TOE environment. Certain Linux modules have been altered to provide specialized functionality for ASG. In addition, the TOE also comprises security enforcing packages created by Astaro. Therefore, the TOE comprises the following packages:

- iptables-1.3.1-13.i686.rpm
- netfilter-tools-6.1-11.i686.rpm

- syslog-ng-1.6.7-7.i686.rpm
- ulogd-1.23-9.i686.rpm
- ep-aua-6.2-67.i686.rpm
- ep-webadmin-6.3-88.i686.rpm

5 The Linux OS is automatically hardened and configured by the installation scripts of the ASG software. Whereas the configuration scripts and their effect are part of the TOE, the services and files configured are, with the above exceptions, part of the TOE environment.

3 TOE Security Environment

10 ## 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
15 internal and external networks is equivalent. The language is clearly aimed at government environments.

ASG Software is 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
20 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

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

A.PHYSEC	The TOE is physically secure.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
30 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.
35 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.

3.1.3 Additional Assumptions

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

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.

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 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's 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.
T.PROCOM	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 Threats to be Addressed by the Operating Environment

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

T.TUSAGE	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 Organizational 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 organizational security policies are included.

4 Security Objectives

4.1 Security Objectives for the TOE

4.1.1 Security Objectives for the TOE Listed in the TFFWLR PP

5 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.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.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.

For a detailed mapping between threats and the IT security objectives listed above see Section 8.1 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 according to 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 “OE.x” are stated below. The TFFWLR PP includes two security objectives, OE.GUIDAN and OE.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.

OE.PHYSEC	The TOE is physically secure.
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.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.
OE.PUBLIC	The TOE does not host public data.
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
OE.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.
OE.NOREMO	Human users can not access the TOE remotely from the internal or external networks.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.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.

4.2.2 Additional Security Objectives for the Environment

In addition to the objectives listed above, this ST defines the following additional objectives for the TOE environment. The first objective addresses the fact that administration is only possible via a directly attached console and not via remote connections. The other objectives have been introduced because some of the SFRs have been moved to the environment (because some of the the security functions are either provided or supported by the TOE's underlying operating system), and therefore require the objectives for the environment to be stated.

OE.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.
OE.MEDIAT	The TOE environment must ensure the data flow between the TOE and the external network interfaces and that no residual information from an information flow through the TOE is leaked by the TOE environment.
OE.SELPRO	The TOE environment must support the TOE's self-protection by not allow tampering, bypassing or deactivation of the TOE security functions through the TOE environment.
OE.TIME	The TOE environment must be able provide reliable time stamps to the TOE on the TOE's request.

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 2. 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.

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. 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
FAU_SAR.1	Audit review	
FAU_SAR.3	Selectable audit review	
FAU_STG.1	Protected audit trail storage	
FAU_STG.4	Prevention 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

CC Part 2 Security Functional Components		
Identifier	**Name**	**Notes**
		FMT_MOF.1 references to this component.
FIA_ATD.1	User attribute definition	
FIA_SOS.1	Specification of secrets	
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	
FMT_SMR.1	Security Roles	
FPT_RVM.1	Non-bypassability of the TSP	Parts of the function are realized in the TOE's IT environment
FPT_SEP.1	TSF domain separation	Parts of the function are realized in the TOE's IT environment

Table 2: 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 probabilistic 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 requirement:

FIA_SOS.1 The password complexity required by FIA_SOS.1 can be demonstrated to have a strength of function so 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[3] specified in Table 3; and

c) [the event in Table 3 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 identities, 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 3].

Functional Component	Level	Auditable Event	Additional Audit Records Contents
FDP_IFF.1	Basic	All decisions on request for information flow	The presumed addresses of the source and destination subject
FIA_UAU.1	Basic	Any use of the authentication mechanism	The user[4] identities provided to the TOE
FIA_UID.2	Basic	All use of the user identification mechanism	The user[5] 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	The identity of the authorized administrator performing the modification and the

[3] The wording for this requirement was taken from the PP. CC V2.2 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. The CC uses the level „minimum“, which is called „minimal“ in the PP, and has then refined the requirement with a higher level of audit in some cases.
[4] User in this context corresponds to the administrator.
[5] User in this context corresponds to the administrator.

Functional Component	Level	Auditable Event	Additional Audit Records Contents
		administrator role	user identity being associated with the authorized administrator role
FPT_STM.1	Minimal	Changes of the time	The identity of the authorized administrator performing the operation and the new time

Table 3 Auditable Events

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[6]

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] modifications to the audit records.

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*] 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:

[6] Since there is no access to the audit trail storage via the web console the role of the operating system is of no relevance here.

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].

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 subject[7] 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;

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

- 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 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.]

Application Note: 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. A "service", listed in FDP_IFF.1.1(b), could be identified, for example, by a source port number and/or destination port number.

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[8]:

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.

d) authentication data]].

[8] User in this context corresponds to administrator.

5.1.2.10 FIA_SOS.1 Specification of secrets

FIA_SOS.1 The TSF shall provide a mechanism to verify that secrets meet [the following requirements concerning length and complexity:

- minimum length of eight (8) characters
- use of lower-case characters
- use of upper-case characters
- inclusion of one or more numerical digits
- inclusion of special characters (all of which must be within the range of 32 to 126 of the ASCII character table)

for administrators accessing the TSF via the GUI interfaces].

5.1.2.11 FIA_UAU.1 Timing of authentication

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

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

5.1.2.12 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Application Note: the term “user” applies only to administrators identifying and authenticating themselves through the WebAdmin GUI on the protected console. There are no other users known to the TOE.

5.1.2.13 FMT_MOF.1 Management of security functions behavior[9]

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

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

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;

~~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].

5.1.2.14 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].

5.1.2.15 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.

5.1.2.16 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 flow;

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.]

5.1.2.17 FMT_SMR.1 Security Roles

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

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

5.1.2.18 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.

5.1.2.19 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.

5.2 TOE Security Assurance Requirements

The target evaluation assurance level for ASG Software is EAL2 [CC] augmented by ALC_FLR.1.

5.3 Security Requirements for the IT Environment

The TOE makes use of parts of the Linux operating system, which is part of ASG software, but considered to be in the TOE environment for the purpose of this evaluation (see section 6.1 “ASG Architecture”).

In order to provide its security functions properly, the TOE relies on some security functions provided by parts of the Linux system in the IT environment. These functions are listed in the following subsections.

Note that ASG Software is built on the SLES9 Linux distribution, which has been successfully evaluated at EAL4 as meeting the security functional requirements stated below. Therefore, some amount of trust can be placed on the IT environment to provide the required security functions.

5.3.1 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.

Application Note: The Linux operating system ensures due to its internal memory management that all processes can only use their own respective memory spaces.

5.3.2 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.

Application Note: The TOE's interfaces are not directly invoked by packages arriving at a network interface. The IT environment must therefore ensure that these packets are handed off to the TOE for inspection and policy decisions.

5.3.3 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.

5.3.4 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: 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.

6 TOE Summary Specification

This section provides:

(a) a description of the ASG architecture.

(b) 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 9. The assurance measures and assurance requirements are cross-referenced in Table 10.

6.1 ASG Architecture

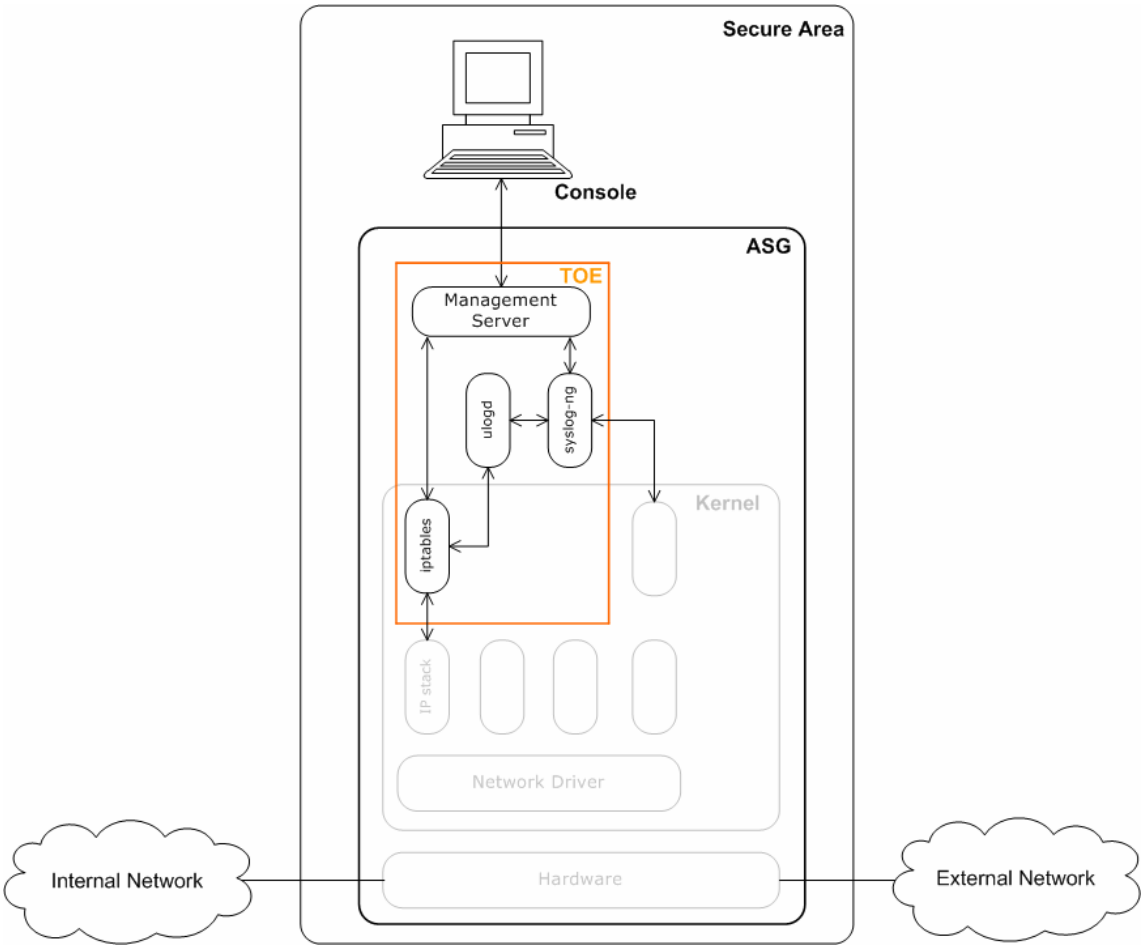

Figure 2 ASG Architecture

Figure 2 shows the overall architecture of the Astaro Security Gateway. The TOE that has been subject to this evaluation encompasses the core firewall functionality and its management components:

6.1.1 Management Server

The Management server consists of a set of web pages and CGI scripts that provide the GUI to the administrator working at the locally attached console, and translate the administrator's actions initiated at this GUI into the appropriate commands and configuration file updates in the ASG. Administrator actions may affect the TOE itself (e.g. when changing firewall rules or viewing audit logs), or the runtime environment (e.g. when setting the system's clock).

The HTTP service itself is provided by an Apache2 web server, which is not part of the TOE, but belongs to the TOE environment.

6.1.2 Kernel Components

The following section briefly introduces the major ASG component associated with the kernel. Note that this component usually consists of a module attached to the Linux kernel, as well as additional userspace commands or daemons.

netfilter/iptables

The packet filtering and NAT functionality of ASG is provided by the iptables module of the kernel. Based on the standard iptables component of the Linux Kernel, Astaro has modified this component to provide a more robustness and better performance. In addition to the kernel module, this component also provides the iptables userspace command necessary to configure all aspects of the kernel module.

Furthermore, iptables is considered an additional (logical) interface to the TOE through which the IP packets arrive at the TOE, i.e. the TOE receives IP packets by means of a set of hooks within the IP stack of the Linux kernel for intercepting and manipulating IP packets.

6.1.3 Logging Components

The following list briefly introduces the major ASG components associated with logging.

Ulog

ulogd is the userspace logging daemon for all netfilter/iptables related logging. It is part of the netfilter/iptables framework.

syslog-ng

The standard syslog-ng is required for all logging and has been added to the TOE because it has not yet been part of an evaluation of Linux.

6.1.4 TOE Environment

ASG uses a standard Linux kernel to provide the basic operating system functionality. ASG is based on the SuSE Linux Enterprise Server version 9 (SLES9) distribution, which has already been successfully evaluated at the Common Criteria assurance level EAL4.
The main differences between the already evaluated components and the components distributed by ASG are as follows:

- ASG only includes only the components absolutely necessary to support the ASG functions
- During installation, the components are automatically configured in a secure manner.
- Some components not relevant to security have been modified to tailor the system to its special purpose as a security gateway rather than a general-purpose computing system, and to enhance its performance.

6.2 TOE Security Functions

The security functional requirements stated in section 5.1 are implemented by a set of security functions of the TOE:

F.HMI — The TOE provides the administrator with the capability to perform Human-Machine-Interface (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 3.

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 3.

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 and issuing warning messages when certain thresholds are reached.

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. service; and

V. 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 administrators only. 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 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 by a password 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): The administrator is required to choose a password with the following characteristics:

- minimum length of eight (8) characters
- use of lower-case characters
- use of upper-case characters
- inclusion of one or more numerical digits
- inclusion of special characters (all of which must be within the range of 32 to 126 of the ASCII character table)

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.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. The default TOE policy is to discard packets that are not explicitly allowed by a firewall rule.

6.3 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 authorized changes are made to the TOE configuration items and implemented in the evaluated version of the TOE. The automated CM system also supports the generation of the TOE. 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.

M.GETTOE — The developer uses documented and controlled processes 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 and a high-level TOE design. The informal, internally consistent, functional specification describes the TSF and the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages. The functional specification completely represents the TSF. 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.

M.TRACE — Correspondence mappings demonstrate that the security functionality detailed in the ST can be traced to the interfaces identified in the functional specification (FSP) and to the components in the high-level design (HLD), and between FSP and HLD.

M.DOCS — Documentation is provided in the form of operational guidance for the administrator. 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 behavior 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.

In conformance with the TFFWLR PP application note on AGD_USR, no dedicated user documentation is provided.

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.

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.

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

7 Protection Profile Claims

This section provides the protection profile (PP) conformance claim statements.

7.1 PP Reference

The TOE conforms to the following protection profile:

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

7.2 PP Tailoring

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

The TFFWLR PP considers remote access for administrators to be an option. Although such remote access may be convenient for the administrators, ASG Software in its evaluated configuration does not allow such connections, because this is considered to be the more secure option. All administration of the TOE occurs from a locally connected, physically secure console (see assumption A.CONSOLE).

Therefore, all assumptions, objectives and security functional requirements applicable only to remote administration have been removed from this ST or have been marked as obsolete. By doing so, the ST provides a clearer set of assumptions and objectives to the readers and avoids ambiguities. Note that the assumed threats of the PP remain unchanged, because the TOE counters all of them.

In particular, the following changes were introduced because of the missing remote administration option:

- A.REMACC has been removed, as it cannot be assumed that administrators gain remote access to the TOE. Similarly, the environment objective OE.REMACC has been removed
- The Objective O.SINUSE has been removed. The intent of the objective was to protect administrator sessions over remote connections by a single-use authentication mechanism. With no remote administration possible, this objective is obsolete. The PP rationale maps this to the threats T.REPEAT and T.REPLAY. As single-use authentication mechanisms do not protect against attackers trying guess the secret, the mapping from O.SINUSE to T.REPEAT is wrong anyway. O.SINUSE is the only objective to require FIA_UAU.4, which has been removed from this ST as well.
- The objective O.ENCRYP has been removed. It maps to T.NOAUTH, because unencrypted transmission of passwords for remote administrators would allow an attacker to gain access to the TOE or hijack the administrator session; this cannot occur as there is no remote administration allowed. The mapping to T.PROCOM is also obsolete because the missing remote administration makes the whole threat

obsolete. On the SFR side, FCS_COP maps to this objective, but has been removed from this ST as well.

- The scope of the environment objective OE.NOREMO has been extended to include all users rather than non-administrative users only.
- Security Functional Requirements FIA_UAU.4, FCS_COP.1 and FIA_AFL.1 were omitted because the TOE allows no remote administration, see Table 2 and section 5.1.1.1. As only administrators can log in at the local console, revoking or blocking the account after several authentication failures is not necessary, and, in fact, not desirable.
- FIA_UAU.1 has been changed to remove “authorized external IT entities”, which do not exist in the evaluated configuration.
- FMT_MOF.1: the items d), e), f), g) and l) have been removed, as the TOE supports neither authorized IT entities nor remote administration.
- The rationale was updated to reflect these changes and to connect threats, objectives, assumptions and SFRs according to this ST’s scenario without remote administration.
- Non-applicable rows O.SINUSE and O.ENCRYP were removed from the mapping in Table 4.
- Non-applicable columns O.SINUSE and O.ENCRYP were removed from the mapping in Table 6. As this tailoring had impact on 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.

Other tailoring actions were as follows:

- Requirements that requested ST author input were completed in accordance with the direction given in the TFFWLR PP.
- The threat T.TUSAGE was augmented to cover TOE delivery, thus matching the environment objective OE.GUIDAN.
- The strength-of-function claim in section 5.1.1.2 has been targeted against FIA_SOS.1 rather than

FIA_UAU.1. The authors felt that FIA_SOS.1 is directly concerned with the strength of the password mechanism on which FIA_UAU.1 relies. FIA_SOS.1 is not present in the PP and cannot be the target of such a claim there (although other PPs from the same source do so). The change does not introduce any ambiguity, as there is only one password mechanism protecting the access of administrators at the console.

- 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 requirement FPT_STM.1 was moved into the TOE IT environment section, as the time stamps are provided by the operating system (although the time can be set through the WebAdmin GUI). The part of the PP application note addressing multi-device issues has been removed, as it is not applicable to the TOE and its environment. As the CC require SFRs for the environment to be mapped to an objective for the environment rather than contributing directly to a TOE security objective, OE.TIME was introduced to cover the environment SFR FPT_STM.1
- Section 5.2 claims all EAL2 security assurance requirements (SARs) rather than copying all SARs from the TFFWLR PP. Both lists are identical. The additional application notes have been addressed in this ST.

7.3 TFFWLR PP ADDITIONS

The EAL2 assurance requirements of the TFFWLR PP were added.

FIA_SOS.1 was added as the TOE enforces password complexity rules.

FMT_MSA.1 was added to satisfy the dependency of FMT_MSA.3, although the PP rationale argues that FMT_MOF.1 sufficiently covers the FMT_MSA.1 requirements.

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

FPT_SEP.1 has been stated as an SFR for the IT environment because parts of the functionality necessary to ensure a separated execution domain are provided by the IT environment. For example, memory protection, process separation and the management of user and kernel address space is provided by those parts of the Linux operating system that are considered to be part of the IT environment. The TOE part of

FPT_SEP.1 deals with the ability of the TOE to distinguish between a large number of connections and maintain information on their state. As the CC require SFRs for the environment to be mapped to an objective for the environment rather than contributing directly to a TOE security objective, OE.SELPRO was introduced to cover the environment SFR FPT_SEP.1

FPT_RVM.1 has been stated as an SFR for the IT environment because packets entering the system do not immediately arrive at the TOE's interface. The IP stack needs to dispatch every packet to the TOE security functions in the iptables module for inspection and policy decision. When the TOE has made a policy decision, the IT environment must obey to it and may not send a packet that has been rejected by the TOE to its destination. OE.MEDIAT was introduced as an objective for the environment to cover this environment SFR.

FDP_RIP.1 has been stated as an SFR for the IT environment, because certain functionality required to ensure that no information is made available to unauthorized entities is provided by the parts of the Linux kernel which are in the IT environment, mainly the zeroing of freshly allocated memory. The TOE itself also takes care for the data handled by the TOE functions that no previous information is being made available. The environment objective OE.MEDIAT also covers this SFR.

In response to consumer demand, one assurance requirement, ALC_FLR.1 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 4 provides a bi-directional mapping of Security Objectives to Threats as specified in the TFFWLR PP, tailored by removing 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.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL
O.IDAUTH	X	X								
O.MEDIAT/OE.MEDIAT				X	X	X				
O.SECSTA	X								X	
O.SELPRO/OE.SELPRO	X				X			X	X	X

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL
O.AUDREC/OE.TIME								X		
O.ACCOUN								X		
O.SECFUN	X							X	X	X
O.LIMEXT	X	X	X				X		X	

Table 4 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 requires that users be uniquely identified before accessing the TOE, thus establishing the base for authorization controls.

O.SECSTA ensures that no information is compromised by the TOE upon startup or recovery, which protects against unauthorized access to TOE-protected resources outside “normal” operations.

O.SECFUN requires that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

O.LIMEXT requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions. In the case of ASG, this means that the TOE is configured to prohibit external access for users (i.e. administrators), thus efficiently mitigating this threat.

O.SELPRO provides for an implementation that ensures that the TOE’s security functions cannot be bypassed. OE.SELPRO ensures that bypassing cannot happen through the TOE environment.

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.LIMEXT counters this threat by prohibiting remote access for administrators and therefore avoids to expose any interface to possible attackers who might try to guess an authentication secret.

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.

Note: The rationale for O.IDAUTH has been copied from TFFWLR PP. The ST authors do not believe this objective to counter the threat; rather, the objective itself gives raise to this threat by requiring identification and authentication and therefore make overcoming this obstacle a necessity for an attacker in order to gain access to the TOE's resources. The rationale has been left in this ST because the authors accept that TFFWLR PP has been certified and the rationale has already been investigated thoroughly. Therefore, O.IDAUTH might help to mitigate this threat in ways unbeknownst to the ST authors.

Note: TFFWLR PP also claims that this threat can be countered by a single-use authentication mechanism (O.SINUSE). The ST authors believe this claim to be wrong either, as changing a password after every use does not prohibit an attacker from trying to guess it, but only prohibits re-use of the authentication secret and thus mitigates T.REPLAY.

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

O.LIMEXT effectively counters this threat, as no remote administration is possible. Therefore, no interface visible to possible attackers supports any identification and authentication, so that no interface is provided where a replay attack could be mounted.

The objective O.SINUSE from TFFWLR PP has been deleted in this ST. A single-use authentication mechanism is a commonly accepted way to mitigate the threat of replay attacks. As O.LIMEXT makes such an attack impossible, there is no need to have O.SINUSE as a TOE objective.

The TFFWLR PP also maps O.SECFUN to this threat. The ST authors cannot see how this objective would contribute to counter a replay attack other than by providing security functions for the administration of the TOE, which then allow to configure the system in a way that it meets the objective O.LIMEXT. Therefore, this objective was intentionally not mapped to T.REPLAY.

	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 requires that all information that passes through the networks is mediated by the TOE. OE.MEDIAT supports this by requiring that the TOE environment supports the TOE in passing all information flow to and from external network interfaces to the TOE.
		The security functions implementing O.MEDIAT cannot reliably identify every spoofed source address. Due to the nature of IP addressing, the firewall can only recognize if addresses are in a range that is expected on a certain physical interface. Therefore, O.MEDIATE allows to recognize spoofed packets arriving on the "wrong" interface. The ST authors interpret T.ASPOOF such that this was the intended mitigation, since TFFWLR PP explicitly talks about "perceived addresses" in several other places. This clearly indicates that the PP authors were aware that address spoofing cannot be prevented in every case, but that it must be prevented that outsiders are able to masquerade as insiders.
	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 requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted. OE.MEDIAT ensures that this objective cannot be jeopardized by the TOE environment.
		O.SELPRO ensures that security functions cannot be bypassed, while OE.SELPRO ensures that bypassing cannot occur through the TOE environment.
	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 directly counters this threat by requiring that that no residual information is transmitted; OE.MEDIAT ensures that this cannot happen through the TOE environment either.
	T.PROCOM	*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.

O.LIMEXT effectively counters this threat by eliminating remote access of authorized administrators altogether.

5 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 requires a readable audit trail and a means to search and sort the information contained in the audit trail. OE.TIME supports O.AUDREC by requiring that the environment provides suitable timestamps for the audit records.

O.SECFUN ensures that these functions can be used by authorized administrators.

O.ACCOUN 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.

Note that the TOE only support administrators as users; all other traffic flows without any attribution to a user known by the TOE.

Note also that the TOE cannot enforce that audit trails are being reviewed. This requires appropriate organizational policies implemented in the TOE environment that are outside the scope of this ST.

O.SELPRO ensures that the audit functions provided by the TOE cannot be bypassed, while OE.SELPRO ensures that such bypassing cannot occur through the TOE environment.

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

O.SECSTA ensures that no information is compromised by the TOE upon startup or recovery. Therefore, unauthorized modification of TOE configuration data cannot occur outside “normal” operation.

O.SELPRO requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. Therefore, modification of TSF data (including “critical TOE configuration data”) cannot occur by an unauthorized person. OE.SELPRO ensures that this cannot happen through the TOE environment either.

		O.LIMEXT 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). Note that in this ST, remote access is prevented even for authorized administrators.
		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 requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. This includes deactivation of auditing by exhausting audit trail storage.
		O.SECFUN restricts security functions and their management to authorized administrators. This contributes to the mitigation of this threat as an attacker cannot decrease the size of the audit trail through the management interfaces in order to allow a flooding attack to succeed earlier or to configure the system such that exhaustion of audit trail space would lead to a loss of audit records by allowing security relevant events to occur in this situation.

8.1.2 Environment Security Objectives Rationale

Table 5 provides a bi-directional mapping of security objectives for the environment to assumptions and threats to be countered by the TOE environment (in addition to the environment objectives OE.SELPRO, OE.MEDIAT and OE.TIME, which have been addressed together with their TOE objective counterparts in section 8.1.1). It shows that each of the assumptions and threats 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 and threat is addressed by the corresponding security objective(s).

Note that TFFWLR PP reuses all assumptions as objectives for the TOE environment. The rationale in PP chapter 6.2 only copies the text of the assumptions/environment objectives (only exchanging the prefix "A." by "O."), but fails to provide any clue as to why they are necessary. The only

exceptions are the additional objectives OE.GUIDAN and OE.ADMTRA, which are mapped to T.TUSAGE. The following rationale is therefore an extension to the PP rationale.

	T.TUSAGE	A.PHYSEC	A.LOWEXP	A.GENPUR	A.PUBLIC	A.NOEVIL	A.SINGEN	A.DIRECT	A.NOREMO	A.CONSOLE
OE.PHYSEC	X	X								
OE.LOWEXP			X							
OE.GENPUR	X			X						
OE.PUBLIC	X				X					
OE.NOEVIL						X				
OE.SINGEN							X			
OE.DIRECT								X		
OE.NOREMO	X								X	
OE.GUIDAN	X									X
OE.ADMTRA	X									
OE.CONSOLE	X									X

Table 5 Mapping of Security Objectives Assumptions

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

OE.PHYSEC, OE.NOREMO and OE.CONSOLE ensure that no unauthorized person can gain access to the TOE's administrative functions through the IT environment (O.IDAUTH, O.SECFUN, and O.SELPRO ensure this for attempts through the TOE). Therefore, the threat is reduced to inadvertent actions by authorized persons (i.e. administrators).

OE.GUIDAN – The TOE guidance documentation provides clear instructions to administrators how to install, configure and administer the TOE securely, thus contributing to achieving the objective that the TOE must be delivered, installed, administered, and operated in a manner that maintains security. Therefore, inadvertent errors due to missing guidance information can be ruled out.

OE.ADMTRA - Authorized administrators are trained as to establishment and maintenance of security policies and practices; this ensures that authorized persons (i.e. administrators) will have sufficient knowledge of the guidance information to correctly install, configure and operate the TOE.

OE.GENPUR and OE.PUBLIC ensure that the firewall system is not used for other general purpose computing tasks. This avoids that conflicting configuration and administration (even by possibly other authorized users than the TOE administrators) can take place and that services that could bypass the TOE security functions could be installed.

Note that OE.NOEVIL has not been mapped to this threat, because the threat is only concerned with inadvertent breaches of security by administrative usage. However, the presence of A.NOEVIL/OE.NOEVIL allows this threat to be narrowed down to inadvertent events, as malicious events have been ruled out by this assumption/objective.

A.PHYSEC *The TOE is physically secure.*

OE.PHYSEC directly maps to this assumption. The TOE must be operated in a secure environment, as neither the TOE nor its underlying software and hardware is assumed to be able of protecting themselves against manipulation by direct physical access, e.g. by rewiring network interfaces or exchanging disks.

A.LOWEXP *The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.*

OE.LOWEXP directly maps to this assumption.

Section 3.2.1.1 of this ST already states the following: “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.”. Therefore, this assumption/objective is redundant and can safely be ignored. Since it does not do any harm either, it has been kept for a maximum of consistency to the PP.

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.*

OE.GENPUR maps to this assumption. As discussed above for T.TUSAGE, avoiding any general purpose functionality avoids conflicts and side effects of potentially competing services, as it avoids the threats of any additional vulnerability that they might introduce.

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

OE.PUBLIC maps to this assumption. Similar to A.GENPUR/OE.GENPUR, this avoids the necessity for users to directly access the TOE or its environment. Direct access is thus refined to administrators for the sole purpose of administering the TOE and its IT environment and excludes any threat that might originate form the fact that other users could access the TOE or the TOE environment.

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

Mapped directly by OE.NOEVIL. As stated for T.TUSAGE above, this assumption rules out any threats originating from malicious administrators. As with any IT system based on a model with one super-user that is allowed all access to any resource of the system, this TOE finally cannot protect itself against every case of malicious abuse of the administrator's powers. Therefore, administrators must be trusted ultimately, although they still may make mistakes.

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

Directly mapped by OE.SINGEN. This assumption is essential to ensure that the TOE can do its job. Since the TOE cannot itself enforce that inadequate configuration of the network allows packets to be routed between the controlled networks without passing through the TOE, this must be ensured in the TOE's environment.

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.*

Mapped directly by OE.DIRECT. Human users may not always be authorized administrators, as maintenance technicians or other personnel may also be authorized to enter the physically secured perimeter. Therefore, this assumption/objective cannot ensure that only authorized personnel may attempt to access the TOE. This is ultimately ensured by O.IDAUTH (in combination with O.SELPRO).

A.NOREMO	*Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.*
	Mapped directly by OE.NOREMO. The access to the TOE functions is already covered by the TOE itself (O.LIMEXT). Therefore, this assumption/objective is interpreted in a way that the functionality existing in the TOE's IT environment (e.g. most of the Linux kernel) does not allow any additional access. It is therefore assumed that the only way to directly interact with the TOE is through its own proper interfaces, i.e. through the directly attached console, and through the GUI provided there.
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.*
	Directly mapped by OE.CONSOLE. This assumption/objective provides the necessary, sole administrative access point. It is required as no remote access to the administrative functions of the TOE is allowed. As console, TOE and the connection between them are all considered to be in a physically protected environment, no additional logical protection is required to ensure the integrity for administration. Therefore, O.ENCRYP and O.SINUSE have been omitted from the ST (see also chapter 7.2). This assumption also contributes to OE.GUIDAN, as it supports the secure installation and administration from a trusted console

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements Rationale

Table 6 provides a bi-directional mapping of Security Functional Requirements (SFRs) to Security Objectives. It shows that each of the applicable objectives for the TOE is addressed by at least one of the SFRs and that each of the SFRs addresses at least one of the objectives. The table is followed by a discussion of how the Security Functional Requirements address the Security Objectives.

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMTEXT
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				

Table 6 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. 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 information flow control 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. Note that this SFR has been duplicated for the IT environment, as the TOE relies on functionality provided by the IT

environment to ensure residual information protection; furthermore, the IT environment shall not leak residual information either. 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 passwords have a certain complexity to protect against guessing attacks, thus meeting the quality metrics stated for the strength of function in section 5.1.1.2. 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. Remember that the only logical access to the TOE is through the directly connected console in a secure area, and that the only users recognized are administrators. However, not everybody using the console is necessarily an administrator, and administrators must be distinguished to be able to hold them accountable for their actions. Authentication must occur whether or not the user is an authorized administrator. 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. Note that this SFR has been duplicated for the IT environment to ensure that the TSP cannot be bypassed in the IT environment. This component traces back to and aids in meeting the following objective: O.MEDIAT.

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. Note that this SFR has been duplicated for the IT environment, as the TOE relies on parts of the IT environment to support this functionality. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

Note that this SFR has been moved to the IT environment, because time stamps are provided by the operating system's clock. However, the TOE provides an administrative interface to set the clock and the appropriate auditing for this event as required by FAU_GEN.1. Getting reliable timestamps from the IT environment does not impact the functionality required to meet the objective O.AUDREC, to which this SFR traces back to. FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable.

8.2.2 Security Functional Requirements for the IT Environment Rationale

Table 7 provides a bi-directional mapping of Security Functional Requirements for the TOE Environment to Security Objectives for the TOE Environment for those security objectives that supplement the TOE security objectives. It shows that each of the applicable objectives for the TOE's IT environment is addressed by at least one of the SFRs and that each of the SFRs addresses at least one of the objectives. The table is followed by a discussion of how the Security Functional Requirements address the Security Objectives.

	OE.MEDIAT	OE.SELPRO	OE.TIME
FDP_RIP.1	X		
FPT_RVM.1	X		
FPT_SEP.1		X	
FPT_STM.1			X

Table 7 Mapping of Security Functional Requirements for the TOE Environment to TOE Environment Security Objectives

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. Note that this SFR has been duplicated for the IT environment, as the TOE relies on functionality provided by the IT environment to ensure residual information protection; furthermore, the IT environment shall not leak residual information either. This component traces back to and aids in meeting the following objective: OE.MEDIAT, which supplements the TOE objective O.MEDIAT for the support required from the TOE environment..

FPT_RVM.1 Non-bypassability of the TSP

This component ensures that the TSF are always invoked. Note that this SFR has been duplicated for the IT environment to ensure that the TSP cannot be bypassed in the IT environment. This component traces back to and aids in meeting the following objective: OE.MEDIAT, which supplements the TOE objective O.MEDIAT for the support required from the TOE environment.

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, not even through the TOE's environment. Although it might be argued that the TOE always operates in its own domain, as the TOE is alone on the system and does not have to share its resources with other, non-TOE processes anyway (see A.GENPUR and A.PUBLIC), this SFR is considered to be crucial to the TOE's operation, as TOE processes themselves shall be separated. Note that this SFR has been duplicated for the IT environment, as the TOE relies on parts of the IT environment to support this functionality. This component traces back to and aids in meeting the following objective: OE.SELPRO, which supplements the TOE objective O.SELPRO for the support required from the TOE environment.

FPT_STM.1 Reliable time stamps

Note that this SFR has been moved to the IT environment, because time stamps are provided by the operating system's clock. It ensures that the date and time stamps used by the TOE for stamping audit records are dependable. This component traces back to and aids in meeting the following objective: OE.TIME, which supplements the TOE objective O.AUDREC for the support required from the TOE environment.

8.2.3 Assurance Requirements Rationale

Astaro has decided that the TOE is evaluated at EAL2, augmented with flaw remediation (ALC_FLR.1). This combination is termed EAL2+. 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 EAL2+ includes the vulnerability assessment component AVA_VLA.1, Developer 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.

8.2.4 Rationale for Satisfying Functional Requirement Dependencies

Table 8 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	FPT_STM.1 is provided by the IT environment
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 FMT_MSA.3	Yes Yes	
FDP_RIP.1	None	Yes	
FIA_ATD.1	None	Yes	
FIA_SOS.1	None	Yes	
FIA_UAU.1	FIA_UID.1	Yes	FIA_UID.2 is hierarchical
FIA_UID.2	None	Yes	
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Yes Yes	
FMT_MSA.1	[FDP_ACC.1 or **FDP_IFC.1**] FMT_SMF.1 FMT_SMR.1	Yes Yes Yes	
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes	
FMT_SMF.1	None	Yes	
FMT_SMR.1	FIA_UID.1	Yes	FIA_UID.2 is hierarchical
FPT_RVM.1	None	Yes	
FPT_SEP.1	None	Yes	

Table 8 Security Functional Requirement Dependencies

8.2.5 Rationale for Satisfying Assurance Requirement Dependencies

The TOE is conformant to the assurance requirements for EAL2, as specified in Part 3 of the CC, with the augmentation of ALC_FLR.1. Therefore all dependencies are satisfied.

8.2.6 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 behavior

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.

8.2.7 Rationale for Audit Exclusions

The auditable events associated with FIA_AFL.1 in the TFFWLR PP have been excluded because FIA_AFL.1 has been removed. Remote administration has been excluded and login attempts to the console will not be blocked so as to avoid the administrator being locked out of the system, so there is no event associated to FIA_AFL.1 to be audited.

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 9 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
F.HMI		X	X	X	X				X	X	X	X	X	X		X	X		
F.AUDEVT	X																		
F.AUDINF	X																		
F.AUDRPT		X	X																
F.AUDSTO				X	X														
F.FWRULES						X	X												
F.FWINVOKED							X											X	X
F.ADMIN									X				X	X		X	X		
F.I&A										X	X	X							
F.NORESID								X											
F.INIT															X				

Table 9 Mapping of Security Functions to Security Functional Requirements

FAU_GEN.1 Audit data generation

F.AUDEVT and F.AUDINF 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 the IT environment (see FPT_STM.1) 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, while F.HMI provides the HMI for the administrator to review the data.

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, while F.HMI provides the HMI for the administrator to provide the parameters for sorting and searching and to review the data.

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; F.HMI provides the interface for the management actions.

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. F.HMI provides the interface to issue the warnings and for the interaction with the administrator.

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 in combination with the support from the TOE environment (see FPT.RVM.1 for the TOE environment) 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, supported by the TOE environment (see FDP_RIP.1 for the TOE environment), 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

5 F.I&A satisfies the requirement to authenticate the administrator and ensures that the specific strength of function metrics are met by enforcing a basic password complexity. Changes of authentication secrets are performed through F.HMI.

FIA_UAU.1 Timing of authentication

10 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. F.HMI provides the interface where F.I&A is enforced.

FIA_UID.2 User identification before any action

15 F.I&A satisfies the requirement for each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. F.HMI provides the interface where F.I&A is enforced.

FMT_MOF.1 Management of security functions behavior

F.HMI satisfies the requirement for the TOE to provide the user with the
20 capability to manage the security functions of the TOE through external interfaces. F.ADMIN ensures that management functions are available to authorized administrators only.

FMT_MSA.1 Management of security attributes

F.ADMIN satisfies the requirement to restrict the ability to manage (i.e.,
25 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.

30 FMT_SMF.1 Specification of Management Functions

F.HMI satisfies the requirement to manage the TOE security management functions, while F.ADMIN ensures that those functions are restricted to authorized administrators.

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 supported by the TOE environment (see FPT_RVM.1 for the TOE environment) 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.FWINVOKED supported by the TOE environment (see FPT_SEP.1 for the TOE environment) 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. Remember also that the whole system is dedicated to the ASG, so that no separation against other domains is required. Separation is necessary that tasks serving different external entities do not interfere with each other, and that those tasks do not tamper with the security domain itself.

8.4.2 TOE Assurance Measure Rationale

Table 10 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 Requirements are addressed by the corresponding Assurance Measures.

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ALC_FLR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
M.ID	X													
M.CMSYS	X													

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ALC_FLR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
M.GETTOE		X												
M.SETUP			X											
M.SPEC				X	X									
M.TRACE						X								
M.DOCS							X	X	X					
M.FLAWREM									X					
M.TESTCOV										X				
M.DEVTEST											X			
M.INDTEST												X		
M.SOFA													X	
M.VULANAL														X

Table 10 Mapping of Assurance Measures to Assurance Requirements

ACM_CAP.2 Configuration items

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: M.ID provides for unique idemtification of the TOE, and M.CMSYS provides for a CM system with automated support that goes well beyond the requirements of the EAL2 assurance level.

ADO_DEL.1 Delivery procedures

M.GETTOE satisfies the requirement for defined delivery procedures by providing a documented and controlled delivery procedure with the ability to detect modifications to the TOE while in transit.

ADO_IGS.1 Installation, generation, and start-up

M.SETUP satisfies the requirement for installation, generation and start-up procedures: The procedures are well-documented, easy to follow (especially with the provision of a “CC button” to automatically perform the bulk of the configuration steps), and result in a secure configuration of the TOE.

ADV_FSP.1 Informal functional specifications

M.SPEC satisfies the requirement for informal functional specifications: it provides for a document with the informal, consistent and complete specification of the TOE's TSF and their associated interfaces.

ADV_HLD.1 Descriptive high-level design

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

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 by providing the required mappings between the ST and the FSP, ST and HLD, and between FSP and HLD.

AGD_ADM.1 Administrator guidance

M.DOCS satisfies the requirement for administrator guidance documentation. The administrator guidance covers all aspects for the secure operation of the TOE, providing guidance for all administration tasks, descriptions of the appropriate attributes and values, and tips and warnings about possible security pitfalls where appropriate.

AGD_USR.1 User guidance

M.DOCS satisfies the requirement for user guidance documentation. Note that the only users of the TOE are administrators, and therefore user and administrator guidance are the same.

ALC_FLR.1 Basic flaw remediation

M.FLAWREM satisfies the requirement for systematically accepting and remediating security flaws. The procedures established by Astaro ensure that all security flaws are addressed and fixed; they go well beyond the requirements of ALC_FLR.1. M.DOCS provides the documentation required

to enable users to interact with the developers to report flaws and obtain corrections.

ATE_COV.1 Evidence of coverage

M.TESTCOV satisfies the requirement to provide evidence of test coverage by demonstrating the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_FUN.1 Functional testing

M.DEVTEST satisfies the requirement to test the TSF and document the results: Test plans describe how the security functions are tested and that appropriate test scenarios are used, test cases provide the test procedures and their expected results, and the obtained results document that all tests have been performed successfully.

ATE_IND.2 Independent testing – sample

M.INDTEST satisfies the requirement to support independent testing of a selected sample of the developer tests to the extent possible for the developer; independent testing itself is performed by the evaluators and beyond the scope of this ST.

AVA_SOF.1 Strength of TOE security function evaluation

M.SOFA satisfies the requirement for evidence that all TOE security functions have been examined to ensure their strengths against threats as deined by the metric given in the ST. It provides the SOF analysis for the the password mechanism used in F.I&A as the only mechanism suitable for an SOF analysis.

AVA_VLA.1 Developer vulnerability analysis

M.VLA satisfies the requirement to perform and document a vulnerability analysis. The analysis described in M.VLA addresses all threats that the TOE must counter and identifies all relevant vulnerabilities of the TOE, showing that these vulnerabilities cannot be exploited in the TOE's intended operating environment.

8.5 Strength of Function Rationale

ASG Software provides 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 ASG Software can be appropriately protected from physical attacks. ASG Software's management console must be controlled to restrict access to authorized administrators only. It is expected that ASG Software 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 in F.I&A will ensure that the implementation has the required strength.

8.6 TFFWLR PP Claims Rationale

The objective OE.CONSOLE defines how administration is performed. It is additional to the TFFWLR PP claims. This objective was 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 and Abbreviations

	CC	Common Criteria
	CM	Configuration Management
	DMZ	Demilitarized Zone
5	EAL	Evaluation Assurance Level
	FIPS	Federal Information Processing Standard
	FTP	File Transfer Protocol
	FW	Firewall
	GUI	Graphical user interface
10	HMI	Human-Machine Interface
	HTTP	Hypertext Transfer Protocol
	I&A	Identification and Authentication
	I/O	Input/Output
	ID	Identification
15	IP	Internet Protocol
	IPS	Intrusion Prevention System
	IT	Information Technology
	LCD	Liquid Crystal Display
	NAT	Network Address Translation
20	POP3	Post Office Protocol Version 3
	PP	Protection Profile
	SFP	Security Functional Policy
	SFR	Security Functional Requirement
	SMTP	Simple Mail Transfer Protocol
25	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