DataPower XS40 XML Security Gateway
and
DataPower XI50 Integration Appliance
Version 3.6

Security Target Version 0.75

10/09/2008

Prepared for:
IBM SOA Appliance Group
One Rogers St
Cambridge, MA 02142

Prepared By:
IBM/DataPower SOA Appliance Group
&
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is DataPower XS40 XML Security Gateway (XS40) and the DataPower XI50 Integration Appliance (XI50), version 3.6, both developed by DataPower Technology, Inc. of Cambridge, MA. DataPower is a wholly-owned subsidiary of IBM. The XS40 and XI50 are network devices that provide Application-Level Firewall functionality.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Security Target

ST Version – Version 0.75

ST Date – 10/09/2008

TOE Identification – DataPower XS40 XML Security Gateway and XI50 Integration Appliance Version 3.6

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, ISO/IEC 15408.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.3, August 2005, ISO/IEC 15408-2.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.3, August 2005, ISO/IEC 15408-3.
  - Part 3 Conformant
  - EAL 4
- U.S. Department of Defense Application-level Firewall Protection Profile (ALFWPP) for Basic Robustness Environments, Version 1.0, June 22, 2000.

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parenthesis placed at the end of the component. For example FDP_IFC.1(1) and FDP_IFC.1(2) indicate that the ST includes two iterations of the FDP_IFC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

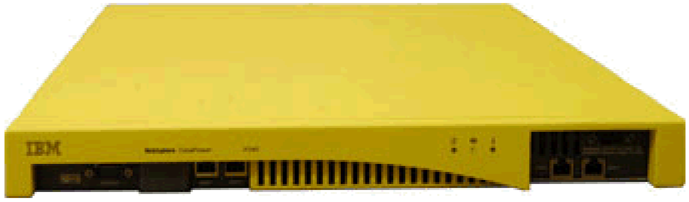
2 TOE Description

The Target of Evaluation (TOE) is the DataPower XS40 XML Security Gateway and the XI50 Integration Appliance, version 3.6 (XS40 and XI50), developed by DataPower Technology, Inc. of Cambridge, MA. DataPower is a wholly-owned subsidiary of IBM. The XS40 and XI50 are network devices that provide Application-Level Firewall functionality. They are hardware enforcement points for Application-Level Firewall policies.

The XS40 and XI50 are separate products, but from the TOE viewpoint are identical except for color; the XS40 is mustard yellow and the XI50 is blue.

2.1 Target of Evaluation (TOE) Architecture

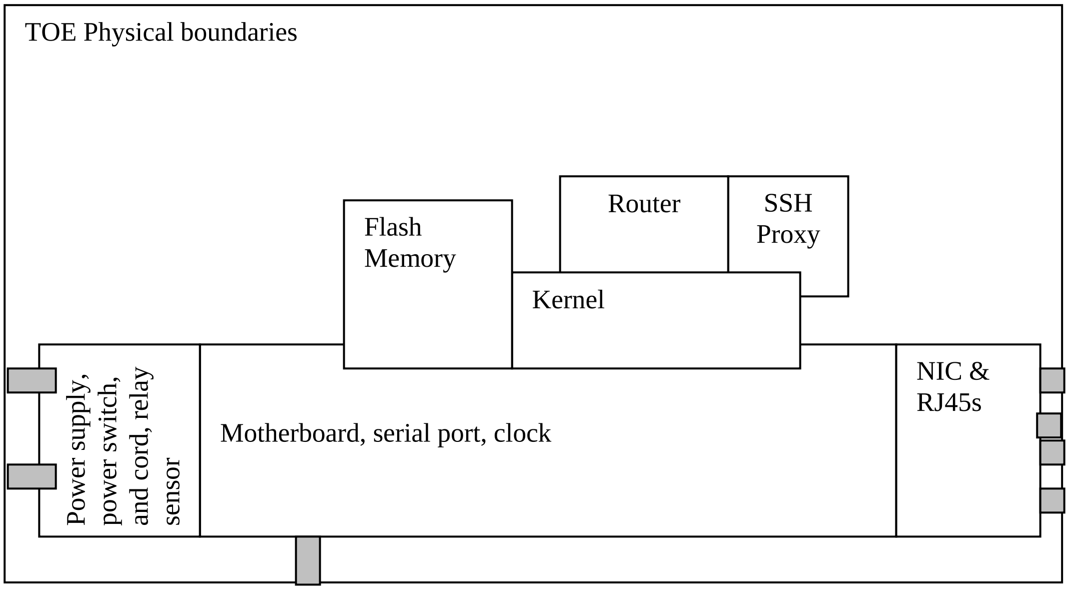
The TOE has the following hardware components: COTS motherboard with a serial communications component, a flash memory component for persistent storage, a power switch, and a "case opened" relay sensor, a clock, and a Network Interface Card (NIC) with multiple ports that provides Ethernet communications functionality. About the ports: The NIC provides four RJ45 ethernet external ports used for data communications. The motherboard also provides one RJll serial external port, which is the administrative interface. Here's a photo of an XS40 device.



The appliance software is the TOE application, the "Router", running on top of a proprietary embedded operating system.

2.1.1 TOE Physical Boundaries

The physical boundaries of the TOE consist of the hardware components and the software combination of the Router and the embedded operating system (OS). The Router, a single application, is actually partitioned over two processes. One, the actual Router process, provides the policy-controlled HTTP proxy functionality and administrative operations; the other, called "the watchdog", starts the Router process and ensures that it is running. The watchdog process restarts the Router process in case of a crash. The software combination of the Router process and the OS controls all administrator interaction and all data-flow on- and off-device. We show a diagram of the physical boundaries directly below.


TOE Physical boundaries
Flash Memory
Router
SSH Proxy
Kernel
Power supply, power switch, and cord, relay sensor
Motherboard, serial port, clock
NIC & RJ45s

On power-up, the hardware boots the embedded operating system. At the end of its standard startup procedure, the the system starts the Router.

Administration is performed using a console connected directly to the TOE's serial port. The administrator uses the TOE's command line interface language (CLI) to administer the TOE. Note that the TOE does not include functionality that would allow for secure remote administration. Remote administration is disallowed.

2.1.2 TOE Logical Boundaries

The logical boundaries consist of the security functions implemented at its external interfaces. They include:

2.1.2.1 Security Audit

The TOE records security relevant events that occur within its scope of control. These events are associated with individual administrators and the audit log can be reviewed by both privileged and authorized administrators.

2.1.2.2 User Data Protection

The TOE allows authorized administrators and privileged administrators to configure policies that are used to control the flow of network traffic based on a variety of attributes including presumed source address, presumed destination address, and transport layer protocol. The Administrative Guidance recommends that only authorized administrators configure information control policies.

2.1.2.3 Identification and Authentication

The TOE maintains administrator accounts that include administrator identity (administrator name and password) and role attributes. The TOE identifies and authenticates administrators using the administrator name and password. Administrators are allowed to access TOE functions only if they are successfully identified and authenticated. The TOE tracks the number of authentication attempts and after a configured number of failures from a privileged administrator disables that account. Disablement prevents any use of that account for operations on the TOE. The account is reset (re-enabled) under control of a privileged administrator. (The TOE includes no "user" accounts. Any reference to "user" in the customer documentation should be construed as meaning "administrator".)

2.1.2.4 Security Management

All management functions including defining and modifying administrator accounts including changing an administrator password, setting the time clock, specifying the limits for number of authentication failure attempts, configuring the audit functions are restricted to privileged administrators. Defining and modifying the information flow control rules is permitted to privileged administrators but the Administrative Guidance recommends against this. The task of defining and modifying information flow control rules is permitted to an authorized administrator within the domain they are authorized for but is prevented in other domains.

2.1.2.5 TSF Protection

The TOE provides a security domain for its own execution that prevents untrusted entities from accessing its functions. The TOE allows for "application domains"; these constitute security domains for segregated sets of administrators. An administrator can access TOE functions only after successful identification and authentication, and after successful association of the administrator to a role. The TOE then enforces access controls on each administrator action based on role, function, resource, and application domain. Information flow is controlled with well-defined security policies. Additionally, the TOE audits the use of its security-sensitive functions. The TOE has a hardware-based clock for issuance of time stamps.

3 Security Environment

This section includes the threats and policies addressed by the TOE and the assumptions about its environment. All threats, policies and assumptions were taken from the Application Filter Firewall PP.

3.1 Threats

T.ASPOOF An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.

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.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 attackers actions.

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

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

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.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.

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.[1]

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

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

[1] Remote administration is optional in the associated Protection Profile. The TOE only supports local administration of the TOE.

3.2 Policies

P.CRYPTO Triple DES encryption (as specified in FIPS 46-3 [3]) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1) [5]. [2]

3.3 Assumptions

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

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

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

A.PHYSEC The TOE is physically secure.

A.PUBLIC The TOE does not host public data.

A.REMACC Privileged and authorized administrators may access the TOE remotely from the internal and external networks.[3]

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

[2] While the associated Protection Profile has a policy for encryption requirements for remote administration, the Protection Profile also explicitly allows this capability to be optional. In the evaluated configuration the TOE does not provide any support for this feature.

[3] While the associated Protection Profile assumes that administrators may access the TOE remotely, the Protection Profile also explicitly allows this capability to be optional. In the evaluated configuration the TOE does not provide any support for this feature.

4 Security Objectives

This section presents the security objectives for the TOE and its Environment. All objectives were taken from the Application Filter Firewall PP.

4.1 Security Objectives for the TOE

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

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.EAL The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.

O.ENCRYP The TOE must protect the confidentiality of its dialogue with a privileged and an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.[4]

O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.

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

O.MEDIAT The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.

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

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.

[4] Remote administration is optional in the associated Protection Profile. The TOE only supports local administration in the evaluation. As such, this objective is included here only for a complete mapping to the Protection Profile since the TOE does not provide any support for this feature.

4.2 Security Objectives for the Environment

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

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

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

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

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

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

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

O.PHYSEC The TOE is physically secure.

O.PUBLIC The TOE does not host public data.

O.REMACC Privileged and authorized administrators may access the TOE remotely from the internal and external networks.[5]

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

[5] Remote administration is optional in the associated Protection Profile. The TOE only supports local administration in the evaluation. As such, this objective is included here only for a complete mapping to the Protection Profile since the TOE does not provide any support for this feature.

5 IT Security Requirements

This section specifies the security functional requirements (SFRs) for the TOE. All SFRs were drawn from Part 2 of the Common Criteria (indirectly via the Protection Profile (PP) identified in Protection Profile Claims section,). Every SFR included in the PP is addressed in this Security Target. Each SFR was changed in this ST to complete operations left incomplete by the PP or to make necessary refinements so that the intent of each SFR remains as specified in the PP. Each SFR was also changed, when necessary, to conform to International Interpretations

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are being satisfied by the TOE. This table, and subsequent sub-sections, was rearranged from the PP as they have been reflected alphabetically.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_SAR.1: Audit Review
	FAU_SAR.3: Selectable Audit Review
	FAU_STG.1: Protected audit trail storage
	FAU_STG.4: Prevention of Audit Data Loss
FDP: User data protection	FDP_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
	FDP_RIP.1: Subset residual information protection
FIA: Identification and Authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	FIA_UAU.1: Timing of authentication
	FIA_UID.2: User identification before any action
FMT: Security Management	FMT_MOF.1(1): Management of security functions behavior
	FMT_MOF.1(2): Management of security functions behavior
	FMT_MOF.1(3): Management of security functions behavior
	FMT_MSA.1(1): Management of security attributes
	FMT_MSA.1(2): Management of security attributes
	FMT_MSA.1(3): Management of security attributes
	FMT_MSA.1(4): Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1(1): Management of TSF data
	FMT_MTD.1(2): Management of TSF data
	FMT_MTD.2: Management of limits on TSF data
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation
	FPT_STM.1: Reliable time stamps

Table 1 TOE Security Functional Components

5.1.1 Security Audit (FAU)

5.1.1.1 Audit Data Generation (FAU_GEN.1)

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 auditable events for the [***not specified***] level of audit; and
c) [**the events listed in the table below**].

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, subject identity, 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 PP/ST, [**information specified in column three of the table below**].

Functional Component	Auditable Event	Additional Audit Record Contents
.FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator or privileged administrator** role.	The identity of the **privileged administrator** performing the modification and the user identity being associated with the authorized administrator **or privileged administrator** role
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.1	Any use of the authentication mechanism.	The user identities provided to the TOE
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the privileged administrator of the user's capability to authenticate.**	The identity of the offending user and the **privileged** administrator
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Changes to the time.	The identity of the **privileged** administrator performing the operation
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the **privileged or authorized** administrator performing the operation

Table 2: Auditable Events

5.1.1.2 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**a privileged and 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.

5.1.1.3 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches* and *sorting***] of audit data based on:
a) [user identity;
b) presumed subject address;
c) ranges of dates;
d) ranges of times;
e) ranges of addresses].

5.1.1.4 Protected audit trail storage (FAU_STG.1)

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***] unauthorized modifications to the audit records.

5.1.1.5 Prevention of Audit Data Loss (FAU_STG.4)

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

5.1.2 User data protection (FDP)

5.1.2.1 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the [**UNAUTHENTICATED SFP**] on:
a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;
b) information: traffic sent through the TOE from one subject to another;
c) operation: pass information].

5.1.2.2 Simple security attributes (FDP_IFF.1)

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**;
- **no additional security 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**;
- **no additional security attributes**].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** 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 information flow security attributes, created by the privileged or authorized administrator;**
- **the presumed address of the source subject, in the information, translates to an internal network address; and**
- **the presumed address of the destination subject, in the information, translates to an address on the other connected network**.

b) **Subjects on the external network can cause information to flow through the TOE to another connected network if:**
- **all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the privileged or 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;**

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;**

e) **The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and**

f) **For application protocols supported by the TOE (e.g., DNS, HTTP, SMTP, and POP3), the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC). This shall be accomplished through protocol filtering proxies that are designed for that purpose**].

5.1.2.3 Subset residual information protection (FDP_RIP.1)

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 [**all objects**].

5.1.3 Identification and Authentication (FIA)

5.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when [**a non-zero number determined by the privileged administrator**] **of** unsuccessful authentication attempts occur related to [**privileged or authorized TOE administrator access or authorized TOE IT entity access**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**prevent the offending user from successfully authenticating until a privileged administrator takes some action to make authentication possible for the user in question**].

5.1.3.2 User attribute definition (FIA_ATD.1)

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

a) **[identity;**

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

c) **no additional security attributes].**

5.1.3.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**information flow in accordance with the UNAUTHENTICATED SFP**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.4 User identification before any action (FIA_UID.2)

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.

5.1.4 Security Management (FMT)

5.1.4.1 Management of security functions behavior (FMT_MOF.1(1))

FMT_MOF.1(1).1 The TSF shall restrict the ability to [***enable, disable***] the functions **[operation of the TOE]** to **[a privileged administrator].**

5.1.4.2 Management of security functions behavior (FMT_MOF.1(2))

FMT_MOF.1(2).1 The TSF shall restrict the ability to [***enable, disable, determine* and *modify the behaviour of***] the functions [

a) audit trail management,

b) backup and restore for TSF data,]

to [**a privileged administrator**].

5.1.4.3 Management of security functions behavior (FMT_MOF.1(3))

FMT_MOF.1(3).1 The TSF shall restrict the ability to [***enable, disable, determine* and *modify the behaviour of***] the functions [

a) backup and restore of information flow rules and audit trail data,

b) communication of authorized external IT entities with the TOE]

to [**a privileged administrator and an authorized administrator**].

5.1.4.4 Management of security attributes (FMT_MSA.1(1))

FMT_MSA.1(1).1 The TSF shall enforce the [**UNAUTHENTICATED SFP**] to restrict the ability to [***delete* attributes from a rule, modify attributes in a rule, add attributes to a rule**] the security attributes [**listed in section FDP_IFF1(1).1**] to [**the privileged or authorized administrator**].

5.1.4.5 Management of security attributes (FMT_MSA.1(2))

FMT_MSA.1(2).1 The TSF shall enforce the [**UNAUTHENTICATED SFP**] to restrict the ability to [***delete* and create**] the security attributes [**information flow rules described in FDP_IFF.1(1)**] to [**the privileged or authorized administrator**].

5.1.4.6 Static attribute initialization (FMT_MSA.3)

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 privileged or authorized administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.7 Management of TSF data (FMT_MTD.1(1))

FMT_MTD.1.1(1) The TSF shall restrict the ability to [***query, modify, delete,* and assign**] the [**user attributes defined in FIA_ATD.1.1**] to [**the privileged administrator**].

5.1.4.8 Management of TSF data (FMT_MTD.1(2))

FMT_MTD.1.1(2) The TSF shall restrict the ability to [**set**] the [**time and date used to form the timestamps in FPT_STM.1.1**] to [**the privileged administrator**].

5.1.4.9 Management of limits on TSF data (FMT_MTD.2)

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [**number of authentication failures**] to [**the privileged administrator**].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF or exceed, the indicated limits: [**actions specified in FIA_AFL.1.2**].

5.1.4.10 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the role**s** [**privileged administrator, authorized administrator**].
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Non-bypassability of the TSP (FPT_RVM.1)

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.

5.1.5.2 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5.3 Reliable time stamps (FPT_STM.1)

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

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 4 augmented with ALC_FLR.1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_AUT.1: Partial CM automation
	ACM_CAP.4: Generation support and acceptance procedures
	ACM_SCP.2: Problem tracking CM coverage
ADO: Delivery and operation	ADO_DEL.2: Detection of modification
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.2: Fully defined external interfaces
	ADV_HLD.2: Security enforcing high-level design
	ADV_IMP.1: Subset of the implementation of the TSF
	ADV_LLD.1: Descriptive low-level design
	ADV_RCR.1: Informal correspondence demonstration
	ADV_SPM.1: Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
	ALC_FLR.1: Basic flaw remediation
	ALC_LCD.1: Developer defined life-cycle model
	ALC_TAT.1: Well-defined development tools
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.2: Validation of analysis
	AVA_SOF.1: Strength of TOE security function evaluation

	AVA_VLA.2: Independent vulnerability analysis

Table 3 EAL 4 augmented with ALC_FLR.1 Assurance Components

5.2.1 Configuration management (ACM)

5.2.1.1 Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1d The developer shall use a CM system.
ACM_AUT.1.2d The developer shall provide a CM plan.
ACM_AUT.1.1c The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.
ACM_AUT.1.2c The CM system shall provide an automated means to support the generation of the TOE.
ACM_AUT.1.3c The CM plan shall describe the automated tools used in the CM system.
ACM_AUT.1.4c The CM plan shall describe how the automated tools are used in the CM system.
ACM_AUT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1d The developer shall provide a reference for the TOE.
ACM_CAP.4.2d The developer shall use a CM system.
ACM_CAP.4.3d The developer shall provide CM documentation.
ACM_CAP.4.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2c The TOE shall be labelled with its reference.
ACM_CAP.4.3c The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
ACM_CAP.4.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.4.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.4.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.4.8c The CM plan shall describe how the CM system is used.
ACM_CAP.4.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.4.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.4.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.4.12c The CM system shall support the generation of the TOE.
ACM_CAP.4.13c The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ACM_CAP.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.3 Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1d The developer shall provide a list of configuration items for the TOE.
ACM_SCP.2.1c The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.
ACM_SCP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Delivery and operation (ADO)

5.2.2.1 Detection of modification (ADO_DEL.2)

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

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

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

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

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

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

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

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

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

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

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

5.2.3 Development (ADV)

5.2.3.1 Fully defined external interfaces (ADV_FSP.2)

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

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

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

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

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

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

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

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

5.2.3.2 Security enforcing high-level design (ADV_HLD.2)

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

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

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

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

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

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

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

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

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

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

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

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

5.2.3.3 Subset of the implementation of the TSF (ADV_IMP.1)

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

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

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

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

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

5.2.3.4 Descriptive low-level design (ADV_LLD.1)

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

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

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

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

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

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

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

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

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

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

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

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

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

5.2.3.5 Informal correspondence demonstration (ADV_RCR.1)

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

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

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

5.2.3.6 Informal TOE security policy model (ADV_SPM.1)

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

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

ADV_SPM.1.1c The TSP model shall be informal.

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

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

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

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

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

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

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

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

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

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

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

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

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

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

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

5.2.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

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

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

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

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

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

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

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

5.2.5 Life cycle support (ALC)

5.2.5.1 Identification of security measures (ALC_DVS.1)

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

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

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

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

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

5.2.5.2 Basic flaw remediation (ALC_FLR.1)

ALC_FLR.1.1d The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.1.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

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

5.2.5.3 Developer defined life-cycle model (ALC_LCD.1)

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

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

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

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

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

5.2.5.4 Well-defined development tools (ALC_TAT.1)

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

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

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

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

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

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

5.2.6 Tests (ATE)

5.2.6.1 Analysis of coverage (ATE_COV.2)

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

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

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

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

5.2.6.2 Testing: high-level design (ATE_DPT.1)

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

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

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

5.2.6.3 Functional testing (ATE_FUN.1)

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

ATE_FUN.1.2d The developer shall provide test documentation.

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

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

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

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

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

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

5.2.6.4 Independent testing - sample (ATE_IND.2)

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

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

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

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

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

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

5.2.7 Vulnerability assessment (AVA)

5.2.7.1 Validation of analysis (AVA_MSU.2)

AVA_MSU.2.1d The developer shall provide guidance documentation.

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

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

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

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

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

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

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

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

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

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

5.2.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

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

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

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

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

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

5.2.7.3 Independent vulnerability analysis (AVA_VLA.2)

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

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

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

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

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

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

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

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

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

AVA_VLA.2.4e The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.2.5e The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

6 TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security Audit

The audit facility records a specific set of events including all required TOE auditable events. The privileged administrator has control over whether information flow decisions are audited or not, however all other audited events are "always on". The privileged administrator can generate audit records of the following event types: system events (shutdown and restart of the device, management events (creating administrator accounts, including associating administrators with roles, changes to the time.) Both the privileged admin and an authorized admin generate audit records of the following event types: Authentication events (use of the identification mechanism, use of the authentication mechanism, reaching of the threshold for unsuccessful authentication attempts);) The TOE itself generates audit records on decisions on requests for information flow based on actual information flow requests and administrator-designated policy.

When the TOE generates an audit record, it contains at least the following:

- Timestamp — date and time of the audit event,
- Event Type — the type of event that is audited,
- Identity – subject identity associated with the audited event, and
- Event Status — success or failure.

The DataPower CLI provides commands for reviewing the audit log. The audit records can be searched or sorted by privileged and authorized administrators by presumed subject address, ranges of dates, ranges of times, and ranges of addresses.

A privileged administrator and an authorized administrator can read the audit records however only the Router software can write to the audit log in any way; it is not directly modifiable by administrators. When the file reaches a specified size, it is renamed to a backup name and a new file is opened. This process is called "log rollover". The Router keeps one rolled-over audit log. At the point when the current audit log fills up and must rollover, the Router will delete the prior rolled-over log if it exists. (Administrators are directed in the Administrative Guidance to regularly archive audit logs in stable off-Router storage.)

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE fulfills this requirement by generating all the required events and including all necessary parameters in the audit records.
- FAU_SAR.1: The TOE fulfills this requirement by providing CLI commands for reviewing the audit log.
- FAU_SAR.3: THE TOE fulfills this requirement by providing CLI commands to search and sort the audit log based on the options specified in this requirement.
- FAU_STG.1, FAU_STG.4: THE TOE fulfills these requirements by not allowing administrators to modify or delete audit records and by providing a mechanism to control loss of audit records if the space available for audit records becomes low.

6.1.2 User data protection

All traffic through the TOE is subject to the information flow policies. The TOE filters traffic based on the following information:

- Presumed address of the source subject

- Presumed address of the destination subject
- Transport layer protocol
- Interface on which traffic arrives and departs
- Service

The authorized administrator has the ability to establish information filtering rules using any combination of the attributes listed to permit or deny a traffic flow. The privileged administrator can also establish these rules but the Administrative Guidance recommends separation of tasks such that the privileged administrator does not establish information flow rules. By default, no traffic is permitted to flow. The TOE mandatorily rejects malformed application protocol (HTTP) requests. Administrators are directed in the Administrative Guidance to create a policy such that the TOE does not accept requests with mismatches between the source address and the TOE interface on which the message arrives. Source addresses on the broadcast or loopback messages as well as messages that specify routing are automatically rejected without any need for an administrator-created policy rules.

The TOE ensures that in all information flows, no residual data is passed. This assurance comes from the fact that all internal objects are initialized when created

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE enforces the UNAUTHENTICATED SFP on all traffic flows.
- FDP_IFF.1: The TOE permits the authorized and the privileged administrator to establish traffic flow rules based on all attributes specified in the requirement. By default, no traffic flows are permitted.
- FDP_RIP.1: The TOE ensures no residual information is shared among entities by initializing all internal objects when created.

6.1.3 Identification and Authentication

When an administrator attempts to access the TOE through the CLI administrator interface, the administrator must provide an administrator name and password at the login dialog. Only privileged administrators and authorized administrators may log into the TOE. Access is only allowed after the TOE verifies the administrator name and password provided against the administrator account database that it maintains. The TOE is configured so that it locks an administrator account after a privileged-administrator-configured number of unsuccessful attempts. Once that number is reached, the administrator cannot login until a privileged administrator resets the locked administrator account.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1: The TOE fulfills this requirement by preventing login of administrators who have reached a defined threshold of unsuccessful authentication attempt.
- FIA_ATD.1: The TOE fulfills this requirement by maintaining administrator accounts that contains administrator identity and role information for individual administrators.
- FIA_UID.2: The TOE fulfills this requirement by preventing administrator access to the TOE until the administrator is successfully identified and authenticated.
- FIA_UAU.1: The TOE fulfills this requirement by preventing administrator access to the TOE until the administrator is successfully identified and authenticated. Network traffic is permitted though the firewall interface but it is submit to the information flow policies.

6.1.4 Security Management

The TOE maintains administrator accounts that contain administrator name, password, and role information. The TOE associates administrators with the appropriate role. The role of "privileged administrator" has the rights to access all TOE functions. Non-privileged administrators have rights to access functions and resources within a "domain" that is designated by a privileged administrator. These functions and resources available in each domain relate only to firewall creation and maintenance, plus the ability to view (but not modify) the system-wide audit log.

The TOE provides privileged administrators with the functions necessary to start, to stop, configure and manage the audit function, including selecting whether events related to information flow are audited. Note that the system automatically audits all other events as defined in FAU_GEN.1, and the user cannot “turn off” auditing of these events. The privileged administrator is also responsible for deleting the rolled over audit log. The current audit log is not delete-able. The TOE also allows the privileged administrator and authorized administrator to observe, search and sort the set of audited events. Note that authorized administrators may also start the audit function since start of the audit function is simultaneous with start up of the TOE via the power switch.

Authorized administrators and privileged administrators are allowed to create and maintain the information flow policy rules that implements the TOE Security Policies, however the Administrative Guidance strongly recommends that only authorized administrators perform these tasks.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1(1): The TOE fulfills this requirements by allowing privileged administrators to shutdown the TOE. Startup of the TOE is by physical access to the power switch.
- FMT_MOF.1(2): The TOE fulfills this requirement by restricting management of the audit function to privileged administrators, and by making sure that only privileged administrators can backup and restore TSF data.
- FMT_MOF.1(3): The TOE fulfills this requirement by restricting management of information flow rules to privileged and authorized administrators by making sure that both roles can enable, disable, determine and modify the behaviour of the communication of authorized external IT entities with the TOE. The TOE further fulfills this requirement by allowing both privileged and authorized administrators to back up and restore information flow rules, and backup audit data. The TOE does not permit audit data to be restored as the current audit log.
- FMT_MSA.1: The TOE fulfills this requirement by allowing a privileged or authorized administrator to create and modify the information flow policy rules.
- FMT_MSA.3: The TOE fulfills this requirement by ensuring that both inbound and outbound information is denied by the TOE until the default values are modified by a privileged or an authorized administrator.
- FMT_MTD.1.1(1) - The TOE fulfills this requirement by restricting access to individual administrator accounts to an administrator who has the privileged role.
- FMT_MTD.1.1(2) - The TOE fulfills this requirement by restricting time-setting functions to a privileged administrator.
- FMT_MTD.2.1 - The TOE fulfills this requirement by only allowing an administrator who has the privileged role to set the login failure threshold.
- FMT_MTD.2.2 - The TOE fulfills this requirement by locking out an administrator who has exceeded the login failure threshold until the account is reset by an administrator who has the privileged role.
- FMT_SMR.1: The TOE fulfills this requirement by maintaining privileged and authorized administrator roles, and associating administrators with the role.

6.1.5 Protection of the TSF

The TOE provides a security domain for its own execution that prevents untrusted entities from accessing its function. It also provides no access to the underlying operating system file system which provides the persistent store for TOE internal objects. In addition, control of physical access is provided by assumptions. The TOE allows for "application domains"; these constitute security domains for segregated sets of administrators. An application domain gives control of its resources to its specific administrators; these administrators cannot access the resource of other domains. The TOE creates a new internal firewall proxy for each external IT client connection thus ensuring separation. Administrators can access TOE functions only after successful identification and authentication, and after successful association of an administrator to a role. The TOE then enforces access controls on each administrator action based on role, function, resource, and application domain. All information flow in the TOE and all access to the TOE functions are protected by enforced access controls. Information flow is controlled with well-defined security policies rules. The TOE also audits the use of its security-sensitive functions. The TOE has a hardware-based clock for issuance of time stamps.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_RVM.1: The TOE fulfills this requirement by making sure that all applicable access checks are made for all administrator operations and for all information flow decisions.
- FPT_SEP.1: The TOE fulfills this requirement by ensuring that the TOE cannot be accessed by untrusted subjects, by ensuring that that authorized administrators can access their application domains but no others, while privileged admins can access all domains. The requirement is further fulfilled by creating a separate internal firewall proxy for each external IT client connection.
- FPT_STM.1: The TOE fulfills this requirement by maintaining the correct time, using the time clock in the hardware appliance.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by DataPower ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. DataPower ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated configuration item modifications are properly controlled. DataPower performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are documented in:

- XS40 XML Security Gateway and XI50 Integration Appliance - Configuration Management Plan

The Configuration management assurance measure satisfies the following EAL 4 assurance requirements:

- ACM_AUT.1
- ACM_CAP.4
- ACM_SCP.2

6.2.2 Delivery and operation

DataPower provides delivery documentation and procedures to identify the TOE, to allow for detection of unauthorized modifications of the TOE, and to guide installation and generation. DataPower's delivery procedures describe all applicable procedures to be used to detect modification to the TOE. DataPower provides documentation that describes the steps necessary to install the TOE in accordance with the evaluated configuration. DataPower provides documentation and procedures to guide configuration for secure network-based administration if that is desired.

These activities are documented in:

- X-Series XML Network Device Installation Guide
- XS40 XML Security Gateway and XI50 Integration Appliance - Delivery and Operation Guide
- XS40 XML Security Gateway and XI50 Integration Appliance – Secure Deployment Guide

The Delivery and operation assurance measure satisfies the following EAL 4 assurance requirements:

- ADO_DEL.2
- ADO_IGS.1

6.2.3 Development

DataPower has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; a low-level design that further decomposes the TOE architecture into modules and describes each module and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the actual implementation of the TOE. Furthermore, DataPower has a security model that describes each of the security policies implemented The TOE. Of course, the implementation of the TOE itself is also available as necessary.

These activities are documented in:

- XS40 XML Security Gateway and XI50 Integration Appliance - Functional Specification
- XS40 XML Security Gateway and XI50 Integration Appliance - High-level Design
- XS40 XML Security Gateway and XI50 Integration Appliance - Low-level Design
- XS40 XML Security Gateway and XI50 Integration Appliance - Design Correspondence Analysis
- XS40 XML Security Gateway and XI50 Integration Appliance - Security Policy Model

The Development assurance measure satisfies the following EAL 4 assurance requirements:

- ADV_FSP.2
- ADV_HLD.2
- ADV_IMP.1
- ADV_LLD.1
- ADV_RCR.1
- ADV_SPM.1

6.2.4 Guidance documents

DataPower provides administrator guidance on how to utilize the TOE security functions and warnings to administrators about actions that can compromise the security of the TOE.

These activities are documented in:

- XS40 XML Security Gateway CLI Reference Guide Volumes I, II, III, and III Release 3.6
- XI50 XML Integration Appliance CLI Reference Guide Volumes I, II, III, and III Release 3.6[6]
- XS40 XML Security Gateway and XI50 Integration Appliance - Secure Deployment Guide 3.6

The Guidance documents assurance measure satisfies the following EAL 4 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

[6] The XS40 and XI50 CLI References guides are equivalent with respect to TOE functions.

6.2.5 Life cycle support

DataPower ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan. DataPower includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. DataPower achieves this through the use of a documented model of the TOE life cycle and well-defined development tools that yield consistent and predictable results.

These activities are documented in:

- XS40 XML Security Gateway and XI50 Integration Appliance - Life-cycle Plan

The Life cycle support assurance measure satisfies the following EAL 4 assurance requirements:

- ALC_DVS.1
- ALC_FLR.2
- ALC_LCD.1
- ALC_TAT.1

6.2.6 Tests

DataPower has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. DataPower has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- XS40 XML Security Gateway and XI50 Integration Appliance - Test Plan
- XS40 XML Security Gateway and XI50 Integration Appliance - Test Coverage Analysis
- XS40 XML Security Gateway and XI50 Integration Appliance - Test Results

The Tests assurance measure satisfies the following EAL 4 assurance requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

The TOE administrator guidance documents describe the operation of the TOE and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator references. Furthermore, DataPower has conducted a misuse analysis demonstrating that the provided guidance is complete.

DataPower has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-Medium.

DataPower performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- XS40 XML Security Gateway and XI50 Integration Appliance - Vulnerability Analysis

The Vulnerability assessment assurance measure satisfies the following EAL 4 assurance requirements:

- AVA_MSU.2
- AVA_SOF.1
- AVA_VLA.2

7 Protection Profile Claims

The TOE conforms to ALFWPP.

This Security Target includes all of the assumptions and threats statements described in the PP, verbatim with the exception of A.REMACC.

This Security Target includes all of the Security Objectives from the PP, verbatim with the exception of O.REMACC.

This Security Target includes all of the Security Functional Requirements from the PP verbatim, except as noted below. Also, this Security Target includes all of the Security Assurance Requirements for EAL4 instead of EAL2, as specified in the PP.

Requirement Component	Modification of Security Functional Requirements
FAU_GEN.1	*Assignment* – completed the assignment (table reference updated).
FAU_SAR.1	No changes.
FAU_SAR.3	No changes.
FAU_STG.1	No changes.
FAU_STG.4	No changes.
FCS_COP.1	*Removed* – the requirement was removed from the ST since remote administration is not supported.
FDP_IFC.1(1)	*Assignment* – completed the assignment.
FDP_IFC.1(2)	*Removed* – the requirement was removed from the ST since the TOE does not support FTP or Telnet through it using an authenticated SFP that would require authentication.
FDP_IFF.1(1)	*Assignment* – completed the assignment, including replacing reference to FIA_UAU.5 with FIA_UAU.1.
FDP_IFF.1(2)	*Removed* – the requirement was removed from the ST since the TOE does not support FTP or Telnet through it using an authenticated SFP that would require authentication.
FDP_RIP.1	No changes.
FIA_AFL.1	No changes.
FIA_ATD.1	*Assignment* – completed the assignment.
FIA_UAU.5	*Replaced* – the requirement was removed from the ST and replaced with FIA_UAU.1 since only a single reusable password mechanism for administrators is supported.
FIA_UID.2	No changes.
FMT_MOF.1(1)	*Assignment* – completed the assignment, limited to replacing reference to FIA_UAU.5 with FIA_UAU.1.
FMT_MOF.1(2)	Split into two iterations to account for the authorized and privileged administrator role capabilities.
FMT_MOF.1(3)	From FMT_MOF.1(2) which was split into two iterations to account for the authorized and privileged administrator role capabilities.
FMT_MSA.1(1)	No changes.
FMT_MSA.1(2)	*Removed* – the requirement was removed from the ST since the TOE does not support FTP or Telnet through it using an authenticated SFP that would require authentication.

Requirement Component	Modification of Security Functional Requirements
FMT_MSA.1(3)	No changes.
FMT_MSA.1(4)	*Removed* – the requirement was removed from the ST since the TOE does not support FTP or Telnet through it using an authenticated SFP that would require authentication.
FMT_MSA.3	*Assignment* – completed the assignment, limited to deleting reference to AUTHENTICATED SFP.
FMT_MTD.1(1)	No changes.
FMT_MTD.1(2)	No changes.
FMT_MTD.2	No changes.
FMT_SMR.1	No changes.
FPT_RVM.1	No changes.
FPT_SEP.1	No changes.
FPT_STM.1	No changes.

8 Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

There are no modifications to the security objectives of the PP, with the exception of O.REMACC and O.SINUSE. O.REMACC was simply a restatement of A.REMACC. FIA_UAU.5 which maps to O.SINUSE was removed from the ST since given the TOE does not support remote administration.

The security objective rationale is presented in Section 6.1 and Section 6.2 of the ALFWPP.

All of the assumptions, threats, and security objectives have been reproduced from the IDSSPP to this ST, with the exception of O.REMACC and O.SINUSE, given the TOE does support remote administration.

8.2 Security Requirements Rationale

The security requirements rationale is presented in Section 6.3 of the ALFWPP.

All of the security functional requirements have been reproduced from the ALFWPP to this ST, except as noted below:

The following security functional requirements were added to the ST:

- FIA_UAU.1: Added since only a single reusable password mechanism for administrators is supported.

The following security functional requirements were removed from the ST:

- FCS_COP.1: Removed from the ST since given the TOE does support remote administration.
- FIA_UAU.5: Removed from the ST since given the TOE does support remote administration.

The additional SFRs map to existing objectives as follows:

- FIA_UAU.1: Maps to O.IDAUTH.

8.3 Security Assurance Requirements Rationale

The TOE exceeds all the ALFWPP EAL2 Assurance Requirements as so stated for EAL4.

8.4 Strength of Functions Rationale

The TOE is targeted at a generalized IT environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have a moderate attack potential. As such, a strength of functions claim of ‘medium’ is appropriate for the intended environment. Note that the only applicable mechanisms (i.e., those that are probabilistic or permutational) are related to identification and authentication (FIA_UAU.1).

8.5 Requirement Dependency Rationale

There are no modifications to the security requirements of the PP with the exception of the following additions:

- FMT_SMF.1: Added to address International Interpretation

The above addition does not introduce any additional dependencies.

The requirement dependency rationale is presented in Section 6.5 of the ALFWPP.

8.6 Explicitly Stated Requirements Rationale

This ST does not contain any explicitly stated requirements.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 4 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security Audit	**Cryptographic support**	**User data protection**	**Identification and Authentication**	**Security Management**	**Protection of the TSF**
FAU_GEN.1	X					
FAU_SAR.1	X					
FAU_SAR.3	X					
FAU_STG.1	X					
FAU_STG.4	X					
FDP_IFC.1			X			
FDP_IFF.1			X			
FDP_RIP.1			X			
FIA_AFL.1				X		
FIA_ATD.1				X		
FIA_UAU.1				X		
FIA_UID.2				X		

	Security Audit	Cryptographic support	User data protection	Identification and Authentication	Security Management	Protection of the TSF
FMT_MOF.1(1)					X	
FMT_MOF.1(2)					X	
FMT_MOF.1(3)					X	
FMT_MSA.1(1)					X	
FMT_MSA.1(2)					X	
FMT_MSA.1(3)					X	
FMT_MSA.1(4)					X	
FMT_MSA.3					X	
FMT_MTD.1(1)					X	
FMT_MTD.1(2)					X	
FMT_MTD.2					X	
FMT_SMR.1					X	
FPT_RVM.1						X
FPT_SEP.1						X
FPT_STM.1						X

Table 4 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.